Calhoun
Institutional Archive of the Naval Postgraduate School

Calhoun: The NPS Institutional Archive

DSpace Repository

Theses and Dissertations | 1. Thesis and Dissertation Collection, all items

2007-12

Method or madness federal oversight structures for critical infrastructure protection

Young, Charles P.

Monterey California. Naval Postgraduate School

http://hdl.handle.net/10945/3022

Downloaded from NPS Archive: Calhoun

http://www.nps.edu/library

Calhoun is the Naval Postgraduate School's public access digital repository for research materials and institutional publications created by the NPS community. Calhoun is named for Professor of Mathematics Guy K. Calhoun, NPS's first appointed -- and published -- scholarly author.

Dudley Knox Library / Naval Postgraduate School
411 Dyer Road / 1 University Circle
Monterey, California USA 93943

NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

METHOD OR MADNESS: FEDERAL OVERSIGHT STRUCTURES FOR CRITICAL INFRASTRUCTURE PROTECTION

by

Charles P. Young

December 2007

Thesis Co-Advisors: Letitia Lawson
Roxanne Zolin

Approved for public release; distribution is unlimited

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE			*Form Approved OMB No. 0704-0188*
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington DC 20503.			
1. AGENCY USE ONLY ***(Leave blank)***	**2. REPORT DATE** December 2007	**3. REPORT TYPE AND DATES COVERED** Master's Thesis	
4. TITLE AND SUBTITLE Method or Madness: Federal Oversight Structures for Critical Infrastructure Protection		**5. FUNDING NUMBERS**	
6. AUTHOR(S) Major Charles P. Young			
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000		**8. PERFORMING ORGANIZATION REPORT NUMBER**	
9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A		**10. SPONSORING/MONITORING AGENCY REPORT NUMBER**	
11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.			
12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release; distribution is unlimited.		**12b. DISTRIBUTION CODE**	

13. ABSTRACT (maximum 200 words)

Telecommunications is one of our most critical national infrastructures, enabling many other infrastructure sectors to function. The federal oversight structure for this sector, put in place by the Department of Homeland Security, relies heavily on voluntary cooperation between the public and private sectors. Given that no large-scale disruption of the nationwide telecommunications backbone has occurred, there is no empirical evidence showing the effectiveness of the structure DHS has put in place.

In an effort to gauge the effectiveness of the various existing infrastructure oversight structures, this thesis examines four specific roles assumed by the federal government and their performance in their respective sectors. These roles and sectors are Owner (aviation), Customer (power), Coordinator (local telecommunications), and Regulator (food). Each case is reviewed to determine the effects of the government role on economic impact of the disruption, the time required to restore initial operating capabilities, and the time required to restore full operating capabilities.

The various cases show that the government role has little direct impact on the costs related to infrastructure disruptions. The Regulator role had a negative impact on timelines for both initial and full restoration. The other roles all made positive contributions to both restoration timelines.

14. SUBJECT TERMS Critical Infrastructure Protection, Public-Private Partnership, Dual Mandate, Regulatory Capture, reliability guidelines, restoration requirements prioritization, regulatory enforcement			**15. NUMBER OF PAGES** 75
			16. PRICE CODE
17. SECURITY CLASSIFICATION OF REPORT Unclassified	**18. SECURITY CLASSIFICATION OF THIS PAGE** Unclassified	**19. SECURITY CLASSIFICATION OF ABSTRACT** Unclassified	**20. LIMITATION OF ABSTRACT** UU

NSN 7540-01-280-5500 Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. 239-18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release; distribution is unlimited

METHOD OR MADNESS: FEDERAL OVERSIGHT STRUCTURES FOR CRITICAL INFRASTRUCTURE PROTECTION

Charles P. Young
Major, United States Air Force
B.S., University of Arkansas, 1992
MBA, Wright State University, 1996

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF ARTS IN NATIONAL SECURITY STUDIES
(Homeland Defense and Security)

from the

NAVAL POSTGRADUATE SCHOOL
December 2007

Author: Major Charles P. Young

Approved by: Letitia Lawson
Thesis Co-Advisor

Roxanne Zolin
Thesis Co-Advisor

Douglas Porch
Chairman, Department of National Security Affairs

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

Telecommunications is one of our most critical national infrastructures, enabling many other infrastructure sectors to function. The federal oversight structure for this sector, put in place by the Department of Homeland Security, relies heavily on voluntary cooperation between the public and private sectors. Given that no large-scale disruption of the nationwide telecommunications backbone has occurred, there is no empirical evidence showing the effectiveness of the structure DHS has put in place.

In an effort to gauge the effectiveness of the various existing infrastructure oversight structures, this thesis examines four specific roles assumed by the federal government and their performance in their respective sectors. These roles and sectors are Owner (aviation), Customer (power), Coordinator (local telecommunications), and Regulator (food). Each case is reviewed to determine the effects of the government role on economic impact of the disruption, the time required to restore initial operating capabilities, and the time required to restore full operating capabilities.

The various cases show that the government role has little direct impact on the costs related to infrastructure disruptions. The Regulator role had a negative impact on timelines for both initial and full restoration. The other roles all made positive contributions to both restoration timelines.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

I. INTRODUCTION 1
A. BACKGROUND 1
1. Emergence of Critical Infrastructure Protection 1
2. Cyberspace as an Economic Enabler 2
3. The Public-Private Dilemma 3
B. IMPORTANCE OF THIS RESEARCH 3
C. LITERATURE REVIEW 4
D. METHODOLOGY 7

II. FEDERAL GOVERNMENT AS AN OWNER — 2001 AIRSPACE RESPONSE TO 9-11 9
A. BACKGROUND 9
1. Commercial Aviation 101 9
2. The Federal Government's Role in Overseeing the Sector 10
B. ANATOMY OF AN AVIATION SECURITY BREACH 11
1. Context of the 2001 Airspace Security Breach 11
2. Security Breach Events and Impacts 12
C. CASE ANALYSIS 14
1. Overall Analysis 14
2. The FAA's Dual Mandate 14
3. Impacts of Regulatory Capture 16
4. Cumbersome Coordination between Federal Agencies 17
5. Ability to Close U.S. Airspace 18
6. Analysis Summary 19

III. FEDERAL GOVERNMENT AS A CUSTOMER — 2003 NORTHEAST BLACKOUT 21
A. BACKGROUND 21
1. Electricity 101 21
2. The Federal Government's Role in Overseeing the Grid 22
B. ANATOMY OF A BLACKOUT 23
1. Context of the 2003 Northeast Blackout 23
2. Blackout Events and Impacts 24
C. CASE ANALYSIS 25
1. Overall Analysis 25
2. Guideline Development 25
a. Guidelines Requiring Validation of Computerized Control and Monitoring Systems 26
b. Guidelines for Operator Training and Certification 27
c. Guidelines for Information Sharing Between Reliability Coordinators 27
3. Compliance Evaluation 28
4. Regulatory Focus on Issues Other Than Reliability 28
5. Analysis Summary 29

IV. FEDERAL GOVERNMENT AS A COORDINATOR — 2005 COMMUNICATIONS RESPONSE TO HURRICANE KATRINA 31
A. BACKGROUND 31
1. Commercial Telecommunications 101 31
2. The Federal Government's Role in Overseeing the Sector 32
B. ANATOMY OF A TELECOMMUNICATIONS OUTAGE 34
1. Context of Hurricane Katrina's Telecommunications Impacts 34
2. Telecommunications Infrastructure Events and Impacts 35
C. CASE ANALYSIS 36
1. Overall Analysis 36
2. Coordination of Regulation Waiver Requests 36
3. Coordination of Restoration Requirements 38
4. Analysis Summary 39

V. FEDERAL GOVERNMENT AS A REGULATOR — 2006 E. COLI OUTBREAK 41
A. BACKGROUND 41
1. Food Production 101 41
2. The Federal Government's Role in Overseeing the Sector 42
B. ANATOMY OF A FOOD-BORN ILLNESS OUTBREAK 43
1. Context of the 2006 E. Coli Outbreak 43
2. Outbreak Events and Impacts 44
C. CASE ANALYSIS 46
1. Overall Analysis 46
2. Factors Contributing to Failed Prevention 46
a. Lax Guidance From the FDA 46
b. Weaknesses in the FDA Inspection Program 47
3. Factors Contributing to Slow Outbreak Response 48
a. Cumbersome Record Keeping for Traceback Accountability 48
b. Inconsistent Reporting from State and Local Entities to the CDC 48
4. Analysis Summary 49

VI. CONCLUSIONS AND RECOMMENDATIONS 51
A. SUMMARY OF CASE STUDY VARIABLES 51
B. CONCLUSIONS ON THE IMPACT OF THE GOVERNMENT ROLE 52
1. Impact of Government Role on Cost 52
2. Impact of Government Role on Disruption Duration 52
C. OTHER CONSIDERATIONS/OBSERVATIONS 53
1. An Ounce of Prevention Really is Worth a Pound of Cure 53
2. Let's Not Relearn the Lessons of the Past 54
D. RECOMMENDATIONS FOR FUTURE STUDY 54

LIST OF REFERENCES 55

INITIAL DISTRIBUTION LIST 61

LIST OF TABLES

Table 1. Summary of Case Study Variables 51

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGMENTS

As with most things I've accomplished in my professional career, the true heavy lifting necessary to finish this thesis was done by others. First of all, thanks to my wife Gloria for enduring countless days with an abnormally ill-tempered husband. Thanks for not throwing me out. Thanks also go to my beautiful daughters, Amber and Lauren, who always say just the right things to keep this all in perspective. Bike rides and soccer games helped to provide just the right diversion at just the right time. Special thanks go to my advisors, Dr. Letitia Lawson and Dr. Roxanne Zolin. Without your boundless patience and thoughtful prodding, the few good thoughts I had would never have found the way to the keyboard. I should also thank the fellow second-floor knuckleheads for the daily lunch meetings, where we discussed and solved every existing Air Force management problem…if only The Man would listen. Finally, the biggest thank you goes to the guy who stocks the library vending machines. I would not have made it without the Diet Cherry Coke.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

A. BACKGROUND

1. Emergence of Critical Infrastructure Protection

Literally every branch of the federal government has a responsibility to protect some piece of America's critical infrastructure. These responsibilities were pulled to the top of the priority list in the wake of the September 11, 2001, attacks. While the concept of protecting critical infrastructures is not new, the importance has increased with its linkage to national security and the focus on protecting the homeland. The criticality of infrastructure has been codified in the *National Infrastructure Protection Plan* (2006) and the *National Strategy for the Physical Protection of Critical Infrastructures and Key Assets* (2003).

These documents, totaling some three hundred pages, are meant to coordinate the protection of infrastructures that are critical to the functioning of American society. These infrastructures include things often taken for granted: food and water supplies, banking and financial services, electric power, and emergency services.[1] Each sector is assigned to a specific federal agency for responsibility. As these individual agencies began building their plans, it became apparent that one infrastructure sector was critical to many others. Underpinning all these infrastructures is the bundle of information technology systems and telecommunications networks which President Bush defines as cyberspace.[2]

[1] Department of Homeland Security, *The National Infrastructure Protection Plan*, Department of Homeland Security, Washington, DC, 2006, 17. The entire list of infrastructures and key resources includes some 18 entities. A list of the most common is given to provide a frame of reference to the reader.

[2] Department of Homeland Security, *The National Strategy to Secure Cyberspace*, Department of Homeland Security, Washington, DC, 2003, foreword.

2. Cyberspace as an Economic Enabler

The recognition of cyberspace as a critical infrastructure sector has been hastened by the emergence of cyberspace as a key enabler of our national economy. The information technology industry as a whole provides some three million jobs across the economy, many of which are among the most high-paying jobs available.[3] Furthermore, many sectors of the economy are becoming increasingly reliant on cyberspace. Economists measure the economic impact of cyberspace by looking at two areas: business-to-consumer (B2C) and business-to-business (B2B) transactions. While the overall percentage of retail sales (B2C) transacted via cyberspace in 2004 was only 2%,[4] the B2B volume was over 16% of total business transactions.[5]

The ubiquity of telecommunications infrastructure has allowed many businesses to dramatically reduce their operating costs and completely revamp their business models. In fact, many companies no longer have the capacity or physical resources to conduct business "the old way." The public-sector owned cyberspace infrastructure is not only critical to our national economy, but also to our federal government. Some 95% of DoD communications services are provisioned by commercial providers.[6] One could expect to find equal or greater levels of dependency across other segments of the federal government. Following a disaster, this dependency leaves many government functions at the mercy of restoration processes used by these commercial providers.

---

[3] Bureau of Labor Statistics, Occupational Labor Statistics (May 2005), Department of Labor, http://www.bls.gov/oes/home.htm, accessed Apr. 11. 2007.

[4] U.S. Census Bureau, *Measuring the Electronic Economy*, 2004, http://www.census.gov/econ/www/ebusiness614.htm, accessed Apr. 11, 2007.

[5] Jonathan L. Willis, "What Impact will E-Commerce Have on the US Economy?" U.S. Federal Reserve Bank of Kansas City, 2002, http://www.kansascityfed.org/Publicat/econrev/Pdf/2q04will.pdf, accessed Apr. 11, 2007.

[6] Personal conversations with communications planners at the Defense Information Systems Agency, documented via email on Apr. 28, 2007.

3. The Public-Private Dilemma

The previous paragraphs clearly show the importance of cyberspace to our national economy and security. The criticality of contributions from both the private and public sectors to securing cyberspace is equally clear. However, despite increasing reliance on private sector companies in many critical infrastructure segments, government agencies have been reluctant to try innovative approaches to partner with industry. David Rothkopf, former Deputy Undersecretary of Commerce for President Clinton, suggests that solutions to many homeland defense and anti-terrorism problems are available in the private sector. According to Rothkopf, the limiting factor in developing these solutions is the fact that "most of the critical questions about how to achieve this [necessary] public-private sector cooperation have yet to be asked."[7] This thesis will attempt to address one of these critical questions: How best to structure the relationship between the players to maximize our ability to effectively reconstitute cyberspace infrastructure after a natural or manmade disruption.

B. IMPORTANCE OF THIS RESEARCH

The following literature review shows there is no shortage of research dealing with cyberspace. Leaders in the Department of Homeland Security (DHS) feel that the structures currently in place are adequate to facilitate the private-public sector cooperation necessary for restoration of the cyberspace infrastructure. Cyber infrastructure providers do not share this view, nor do independent government reviewers outside DHS. These differences, coupled with the lack of academic research directly related to the impact of government oversight structures on infrastructure restoration effectiveness, leaves responsible federal agencies with no guidelines for choosing an oversight structure for their sectors. This thesis analyzes recent restoration activities to determine what impact, if any, different oversight structures have had on these sectors.

[7] David J Rothkopf, "Business Versus Terror," *Foreign Policy*, May-June 2002, 58.

C. LITERATURE REVIEW

The President has pointed out that the unique characteristics of cyberspace, coupled with its criticality to our economy and security, demand an unprecedented level of partnership between the public and private sectors. In fact, President Bush says "the cornerstone of America's cyberspace security strategy is and will remain a public-private partnership.[8] Predictably, the direct public and private sector contributors to this partnership could hardly differ more in their evaluations of the adequacy of the current oversight structures. Independent reviews within the federal government have supported the private sector views that a different approach is needed.[9]

The federal government is represented in this new partnership by the Department of Homeland Security, which believes the current oversight structures are appropriate.[10] Executives from industry service providers, a leading industry trade organization, and the Government Accountability Office (GAO) all have more pessimistic evaluations of the budding partnership between government and business in cyber security. The GAO points out that while DHS has published the required planning documents, they do not provide the level of detail necessary for industry partners to cooperate. While acknowledging the difficulty of the task at hand, the GAO predicts that DHS will have a tough time meeting its responsibilities with its current plans.[11]

These sentiments are echoed by senior executives from private-sector service providers and trade organizations in their testimonies to various Congressional committees. Differing frames of reference notwithstanding, three common themes emerged from their testimonies: 1) insufficient funding for dedicated research and development directly related to cyber security; 2) a lack of clearly defined risk

---

[8] *National Strategy to Secure Cyberspace,* foreword.

[9] Government Accountability Office, *Internet Infrastructure: DHS Faces Challenges in Developing a Joint Public/Private Recovery Plan,* Government Accounting Office, Washington DC, June 2006, *2-4.*

[10] Ibid., 68-73.

[11] Ibid., 45-50.

management priorities, which wastes limited resources; and 3) a lack of clearly defined roles for post-disruption reconstitution of the infrastructure.[12]

Given these differing views, there is little doubt that much work remains to be done toward solidifying this new partnership of public and private sector players in cyberspace infrastructure. Fortunately, no large-scale calamity has put this structure to the test. This relative calm has also left those charged with improving the current model with no real-world experience upon which to base any changes.

The history of the federal government's relationship with commercial providers of electronic communications is extensive. Since the first government telegraph lines were sold in 1835, debates over how best to regulate this industry have surfaced repeatedly. The enduring focus of these debate has been how best to foster *competition* amongst the providers (especially new entrants) in order to keep the price of service low for the home consumer in a local market.[13] As a result, this body of work offers very little theoretical insight into the question of how best to organize the players for effective *reconstitution*, since this new priority demands more *cooperation* than competition.[14]

---

[12] Testimonies include U.S. Congress, House Committee on Homeland Security, Subcommittee on Economic Security, Telecommunications, and Cybersecurity, *Future of DHS Cyber and Telecommunications Security, Testimony of Mr. David M. Barron, 13 Sep 2006;* U.S. Congress, House Committee on Energy and Commerce, Subcommittee on Telecommunications and the Internet, *Cybersecurity Protection, Testimony of Mr. Vincent Weafer, 13 Sep 2006;* and U.S. Congress, House Committee on Homeland Security, Subcommittee on Economic Security, Telecommunications, and Cybersecurity, *Future of DHS Cyber and Telecommunications Security, Testimony of Mr. Paul B. Kurtz, 13 Sep 2006.* All were accessed via Lexis/Nexis on 16 Nov 2006.

[13] Robert W. Crandall, *Competition and Chaos: US Telecommunications Since the 1996 Telecom Act,* Brookings Institution Press, Washington, D.C., 2005, 156-171; Robert Britt Horwitz, *The Irony of Regulatory Reform: The Deregulation of American Telecommunications,* Oxford University Press, New York, NY, 1989, 25- 69. Horwitz attributes this focus to the fact that most regulatory agencies we have today were New Deal organizations, created specifically to prevent another economic disintegration like the Great Depression.

[14] For further information regarding this view of regulation, see the following: Macellus S. Snow, *Marketplace for Teleccommunications: Regulation and Deregulation in Industrialized Democracie.,* Amsterdam: Elsevier Science Publishers, 1986, 253-295; Ian Ayres and John Braithwaite, "Partial-Industry Regulation: A Monopsony Standard for Consumer Protection," *California Law Review* 80, 1 (January 1992), 13-52; Anonymous, "U.S. Policy regarding Internet Governance," *The American Journal of International Law,* Vol. 99, No. 1, Jan., 2005, 258-259; Richard Klingler, *The New Information Industry: Regulatory Challenges and the First Amendmen.,* Brookings Institutions Press, Washington, DC, 1996, 44-68; Robert W. Crandall and Kenneth Flamm, eds., *Changing the Rules: Technological Change, International Competition and Regulation in Communications.* The Brookings Institute, Washington, DC, 1989, 238-245.

The deregulation camp offers a similarly strong yet misguided argument for ending government intervention in market operations, particularly in infrastructure segments. Horwitz states that government regulation, as it is applied to infrastructure services, is effectively limited to "economic growth and the free flow of commerce."[15] The collection of essays compiled by Foldvary and Klein extend this argument further by asserting that most markets no longer require government intervention. *The Half-Life of Policy Rationales* posits that the rapid growth of new technologies in all infrastructure sectors has rendered invalid most cases for government intervention in industry; innovation generally enhances the case for free enterprise. This hypothesis is based on the fact the technology has made most markets more efficient (reducing the need for regulation), while simultaneously making them too complex for successful intervention.[16] While these arguments hold during normal operations, things are different following a disaster.

The extensive writing in opposition to government regulation has not been ignored by DHS. *The National Strategy to Secure Cyberspace* makes that point very clearly. The strategy asserts that "federal regulation will not become a primary means of securing cyberspace."[17] No evidence is given for the validity of this choice, nor is there any indication of an alternative approach to convincing industry to provide a level of security or resilience beyond that which the overall market demands.

Fortunately, there is a growing area of research attempting to address alternatives to the regulation-laissez faire dichotomy. In *Governance and Performance,* Heinrich and Lynn compile essays from many sectors attempting to determine the impact of oversight structures on the overall effectiveness of public policy. One of the themes emerging from this collection is that public policy implementation is rapidly moving from a hierarchical model of government directing industry, to a network model of collaboration and mutual

---

[15] Crandall and Flamm, 87.

[16] Fred E. Foldvary and Daniel B. Klein, eds, *The Half-Life of Policy Rationales: How New Technology Affects Old Policy Issues,* New York University Press, New York, NY, 2003.

[17] *The National Strategy to Secure Cyberspace,* 15.

influence.[18] Stanton further links this idea of managing a network of organizations directly to homeland security. He asserts that "the need to manage a nonhierarchical system that includes governments and private-sector organizations is especially pronounced in homeland security. Coordination…is now an imperative."[19] He concludes that despite this recognition, this type of management is "not completely understood either by practitioners or by academics in the field of public administration."[20]

Taken as a whole, the long-running debate of how government should best interact with private sector infrastructure providers seems to leave public administrators with a palette of roles from which they could choose. The most accommodating role is that of a *customer*, where the government simply procures a service provided in the manner deemed most appropriate by the provider. The government could also perform as a *regulator*, establishing the criteria by which a provider is allowed to offer services. Additionally, the government could act as a *coordinator*, striving to guide a group of providers toward consensus goals on a voluntary basis. Finally, the government could be an infrastructure *owner/operator* on its own. In the area of critical infrastructure protection, the government has in fact assumed each of the roles, and perhaps chosen them without any evidence as to which is most applicable to a given infrastructure sector. This thesis will attempt to determine the impact of these alternative oversight roles on the effectiveness of restoration efforts in critical infrastructure sectors.

D. METHODOLOGY

A single case congruence approach is used to analyze recent restoration activities in various critical infrastructure sectors in the United States. Cases have been chosen to reflect the range of roles assumed by the federal government in these sectors. In each case, effectiveness of reconstitution is evaluated by the following criteria: 1) economic

---

[18] Carolyn J. Heinrich and Laurence E. Lynn, Jr., eds, *Governance and Performance: New Perspectives*, Georgetown University Press, Washington, DC, 2002, 238-291.

[19] Thomas H. Stanton, editor, *Meeting the Challenge of 9/11: Blueprints for More Effective Government*, M.E. Sharpe, Inc., Armonk, NY, 2006, 3.

[20] Ibid., 315-316.

impacts of sector downtime; 2) time required for initial sector restoration; and 3) time required for full sector restoration. The cases to be examined include the 2001 Terrorist Attacks against the United States; the 2003 Northeast Electrical Blackout; the 2005 response to Hurricane Katrina; and the 2006 E-coli Outbreak.

II. FEDERAL GOVERNMENT AS AN OWNER — 2001 AIRSPACE RESPONSE TO 9-11

Commercial aviation contributes to our nation's strength in many significant ways. It is a key economic enabler, contributing some $900 billion per year to the national economy,[21] which accounts for over 8% of our gross domestic product.[22] Despite an outstanding safety record, flaws in the aviation security system were exploited on September 11, 2001, to accomplish the worst terrorist attack in U.S. history. This chapter analyzes how the unique relationship between the federal government and this industry contributed, both positively and negatively, to the 2001 attacks and the immediate response to them. While this case study deals with the passenger segment of commercial aviation, there are numerous security and infrastructure protection issues associated with the cargo segment which merit their own focused analysis.

A. BACKGROUND

1. Commercial Aviation 101

Born in America, aviation has long enjoyed a special status here, evolving from science experiment to war machine to economic engine. The industry includes three major components: manufacturing, flight operations, and terminal operations. Terminal operations include both cargo handling and passenger processing. The industry strives to maintain consumer confidence in passenger aviation with a two-pronged approach addressing both safety and security. The safety program focuses on ensuring that commercial aircraft are airworthy, that pilots and maintenance personnel are properly licensed and trained, and that all operations are conducted in a safe manner. Air safety concerns permeate all three major components of the sector. Security, conversely, is

[21] Jeff Griffith, Deputy Director of Air Traffic at the Federal Aviation Administration, testimony to the National Commission On the Terrorist Attacks Upon the United States, June 2004, http://www.9-11commission.gov/hearings/hearing12/griffith_statement.pdf, accessed Nov. 6, 2007.

[22] Bureau of Economic Analysis, "Gross Domestic Product by Year," U.S. Department of Commerce, http://www.bea.gov/national/index.htm#gdp, accessed Nov. 25, 2007. The 2001 figure of $10,128 billion was used to calculate the percentage of GDP contributed by aviation.

focused at the terminal operations component. Passenger and baggage screening were the predominant security measures in place at the time of the 9-11 attacks. As the following section describes, the federal government was and is heavily involved in both the safety and security aspects of this critical infrastructure sector.[23]

2. The Federal Government's Role in Overseeing the Sector

Aviation observers have written that, in practice, aviation security has long operated "as a 'junior partner' to safety and economic efficiency within the airlines, the airports, and the federal government."[24] The Federal Aviation Administration (FAA) plays a dominant role in the security of commercial aviation, overseeing a multi-tiered architecture of security-related processes. The FAA has two avenues for establishing security-related procedures for commercial aviation. Most procedures are implemented via the regulatory rule-making process, which is used by many federal regulators. The rule-making process is collaborative, with the air carriers and airport authorities having many opportunities to comment and recommend changes to proposed procedures and requirements. In cases where quick implementation is necessary, the FAA has a second avenue, the issuance of Security Directives (SDs). These directives are normally used to implement short-term requirements, which will eventually be address through the rule-making process. Prior to 9-11, SDs were used primarily to transmit the existing FBI no-fly lists to air carriers.[25]

Much like the food sector, the aviation sector has processes that are geared to both prevention and response. The FAA itself operates the nation's airspace management system, controlling the movement of all commercial aircraft. Prior to 9-11, the FAA also established minimal security requirements for passenger screening accomplished by air carriers. It also established in-flight procedures for dealing with hijackers, often referred

[23] R. William Johnstone, *9/11 and the Future of Transportation Security*, Praeger Security International, Westport, CT, 2006, 4-23.

[24] Ibid., 2.

[25] Ibid., 24-34.

to as "The Common Strategy."[26] Finally, local airport authorities were required to follow FAA requirements for physical security of airport property and facilities.[27]

In addition to these relationships with the private sector, the FAA also coordinated with other federal agencies on aviation security. It received intelligence information from various organizations, including the Federal Bureau of Investigation, Central Intelligence Agency, and the Department of Defense (DoD). In addition to intelligence provision, DoD has standing agreements to support the FAA with alert aircraft for hijacking response. The effectiveness of these relationships within the federal government became a major issue in the aftermath of 9-11.[28]

B. ANATOMY OF AN AVIATION SECURITY BREACH

1. Context of the 2001 Airspace Security Breach

American aviation security was not, despite the success of the 9-11 hijackings, lacking for efforts to address known terrorist threats. In fact, the security system had undergone a steady evolution in response to numerous security incidents around the world. The rash of Cuba-bound hijackings in the U.S. during the late 1960's started the changes, bringing increased focus on passenger screening for weapons as well as the standard in-flight highjack response of accommodation. Other successful attacks, such as the Pan Am 103 bombing over Scotland, highlighted changes in terrorist tactics and did not go unnoticed in the U.S. Avenues to increase the sector's anti-sabotage capabilities were pursued along with the existing anti-hijacking initiatives.

---

[26] "Staff Statement #4, Working Papers of the National Commission on the Terror Attacks upon the United States, http://www.9-11commission.gov/staff_statements/staff_statement_4.pdf, accessed Nov. 21, 2007. The Common Strategy was developed by the FAA, in conjunction with the air carriers and federal law enforcement. The strategy was based on the history of hijacker behaviors, which basically showed that planes were taken to get hostages as leverage for negotiating demands. Aircrew members were trained to accommodate the hijackers, avoid confrontations, and get the plane on the ground as soon as possible. No training scenarios had been developed to cover a situation where the hijackers were suicidal, or planned to fly the airplane themselves with the intention of using the airplane as a weapon.

[27] Johnstone, 4-23.

[28] Mike Canavan, Associate Administrator for Civil Aviation Security, Federal Aviation Administration, testimony to the National Commission on Terrorist Attacks Upon the United States, May 23, 2003.

Several Congressional and Presidential commissioned studies recommended sweeping changes to aviation security during the 1980's and 1990's. Between 1987 and 2003, the Government Accountability Office issued some fifty reports on aviation security. The common assessment was that most efforts to improve security had been "weak and ineffective." Despite strong congressional prodding and GAO flag-raising, the attention of the FAA and U.S. air carriers remained focused elsewhere.[29] This point was clearly made by the director of the FAA during her 9/11 Commission testimony: "On September 10, we were not a nation at war…we were a nation bedeviled by delays, concerned about congestion, and impatient to move ahead."[30]

2. Security Breach Events and Impacts

From the perspective of the commercial aviation sector, the 9-11 attack can best be examined as four simultaneous hijackings. Given the previously described security structures, the timeline of the hijackings will be discussed in terms of the prevention failures, followed by the response actions. The single source used for this timeline is *The 9/11 Commission Report*, as this document provides a consensus account of the events based on an exhaustive list of primary sources.[31]

The hijackers were ticketed on four transcontinental flights departing from the East Coast heading west. All were processed through the security checkpoints at three airports, and their experiences were similar. Ten of the nineteen were singled out for additional screening during the check-in process. The only impact of this tagging was that their checked baggage was held until their boarding was confirmed. At least four of the hijackers set off metal detectors while passing through security. At the time of the attacks, procedures called for closer manual inspection to discern the cause of the alarm.

---

[29] Thomas A. Birkland, *Lessons of Disaster: Policy Change after Catastrophic Events*, Georgetown University Press, Washington, DC, 2006, 91-92. Birkland argues that the FAA's lack of effectiveness was related to the impacts of regulatory capture, which will be discussed later in this chapter.

[30] Johnstone, 2.

[31] The National Commission on the Terrorist Attacks Upon the United States, *The 9/11 Commission Report*, http://www.9-11commission.gov/report/index.htm, 1-46, accessed Nov. 6, 2007. It should be noted that numerous conspiracy theorists have pointed out inconsistencies in the 9/11 Commission's report. It is left to the reader to review those additional sources and determine their voracity.

Each of these men was individually searched, but none of their weapons were discovered. By 8:00 a.m., all nineteen men had defeated the existing security measures and were onboard their flights.

The first hijacking commenced at approximately 8:15 a.m. aboard American Airlines Flight 11, which struck the North Tower of the World Trade Center at 8:46 a.m. At approximately 8:45 a.m., United Flight 175 was overtaken and flown into the South Tower at 9:03 a.m. The takeover of American Flight 77 occurred at 8:50 a.m.; it crashed into the Pentagon at 9:37. The final hijacking, United 93, began at 9:30 a.m., some 30 minutes after the second plane struck the World Trade Center. This flight crashed in eastern Pennsylvania at 10:02 after passengers, with knowledge of the first two hijackings, fought with the hijackers.

The FAA Command Center in Herndon, Virginia passed word on the Flight 11 hijacking to its headquarters' operations center at 8:32. The military's Northeast Air Defense Sector was informed at 8:37 a.m. Fighter aircraft were airborne at 8:53, some 7 minutes after the first impact with the World Trade Center. FAA Herndon was notified of Flight 175's hijacked status at 9:01, just 2 minutes before it struck the South Tower. The military was informed of the second hijacking just after the impact. Flight 77 flew undetected for 36 minutes, from 8:56 until 9:32. At 9:25 a.m., the FAA Headquarters issued a nationwide ground stop, effectively closing all airspace over the continental U.S. The military was advised of Flight 77 at 9:36, less than 2 minutes before its impact at the Pentagon. Cleveland Control Center controllers declared Flight 93 as hijacked at 9:32 and informed the FAA Headquarters at 9:34. At 9:42, the FAA ordered all airborne flights to land at the nearest airport. The military was notified at 10:07 regarding Flight 93, some 5 minutes after it crashed.

A well-coordinated and well-executed attack, lasting just over two hours, resulted in catastrophic losses in the U.S. Some 2,783 people lost their lives as a direct result of the attacks.[32] All commercial air travel was suspended over the continental U.S. for four days. The National Airspace System gradually reopened, with the last major airport

[32] Federal Bureau of Investigation, *Terrorism 2000-2001,* U.S. Department of Justice, Washington, DC, 2002, 10.

remaining closed until October 7, 2001.[33] The economic impact to the commercial aviation industry of the 4-day closure has been estimated at $1.4 billion.[34]

C. CASE ANALYSIS

1. Overall Analysis

The failures associated with the 9-11 attacks are well and thoroughly documented, as are the heroic actions of numerous individuals who distinguished themselves during the attacks and the immediate aftermath. Sweeping changes have already been made, in both the public and private sectors, to prevent another attack and to improve response capabilities. Narrowing the focus to commercial aviation and the owner/operator role assumed by the federal government highlights several issues that warrant further analysis. This section will discuss the following: 1) the FAA's Dual Mandate; 2) impacts of regulatory capture; 3) cumbersome coordination between federal agencies; and 4) ability to close U.S. airspace.

2. The FAA's Dual Mandate

Since its creation in 1958, the FAA has had as one of its missions "to establish security provisions which will encourage…the maximum use of the navigable airspace…consistent with the national security."[35] These wide-ranging responsibilities became known as the FAA's Dual Mandate. Through the years, shifting priorities given by the FAA to the two aspects of its mandate gave an almost "Jekyll and Hyde" character to the agency's performance. The impact of this dual mandate on aviation security can be seen by looking at two specific attempts to increase security in the 1990s: The Baseline Working Group and the Core Commission.[36]

---

[33] Metropolitan Washington Airports Authority, *History of Ronald Reagan National Airport*, http://www.mwaa.com/_/File/_/history_DCA.pdf, accessed Nov. 19, 2007, 4.

[34] Gail Makinen, *The Economic Effects of 9/11: A Retrospective Assessment*, Congressional Research Service, Washington, DC, 2002, 30.

[35] Johnstone, 30-31.

[36] Ibid.

The first bombing of the World Trade Center in 1993 convinced the FAA leadership that the threat of foreign terrorism in the U.S. was increasing. In 1996, the FAA chartered the Baseline Working Group, comprising federal officials, industry leaders, and public interest groups, to accomplish the following:

> review the threat assessment of foreign terrorism within the United States, consider the warning and interdiction capabilities of intelligence and law enforcement, examine the vulnerabilities of the domestic civil aviation (in particular checked baggage and checkpoint screening), and consider the consequences of a successful attack.[37]

Formation of this group marked a significant departure from the agency's long-standing history of making security policy changes in reaction to actual events. The group recommended numerous security changes, including better passenger pre-screening, more interagency cooperation at the federal level, and increased federal funding of security initiatives. These recommendations were criticized by the Office of Management and Budget for their "unrealistic outlook" on funding availability. This lack of budget support left the FAA with no choice but to try to cajole additional security investments from an industry already in bad shape financially. Further, the industry did not support implementation of stronger security measures if they increased customer wait times or screening costs.[38]

TWA Flight 800 exploded off the New York coast on the day the Baseline Working Group began to meet. This explosion led President Clinton to charter the White House Commission on Aviation Safety and Security, chaired by Vice President Gore, in early 1997. Using much of the Baseline Working Group's initial work, the Gore Commission made similar recommendations. One significant additional recommendation was the call for the FAA to develop a certification program for the passenger screening companies hired by the airlines. While Congress reacted more positively to the Gore Commission's call for increased federal funding in light of the recent tragedy, this

[37] Johnstone, 19.

[38] Ibid., 20-21.

support was short-lived. Funding for most of the recommendations was significantly reduced after the FAA's final report on the TWA explosion revealed that the cause was a mechanical malfunction.[39]

3. Impacts of Regulatory Capture

The shifting focus of federal decision making regarding aviation security is further complicated by the impact of regulatory capture on the FAA. Regulatory capture occurs when a regulatory agency falls under the dominant influence of the industry it is charged with regulating.[40] Some of the decisions made by the FAA indicate it has succumbed to capture to the detriment of the flying public. Two regulatory decisions particularly relevant to the 9-11 attacks will be described to show the impact of captured behavior on aviation security.

Following the Gore Commission, the FAA proposed changes to its primary security regulations. In part, these changes would have required air carriers to "detect and prevent" the carrying of dangerous weapons onboard an aircraft. The air carriers' largest trade organization, the Air Transport Association, submitted comments to the proposed rule change, suggesting that "detect" be changed to "deter." The rationale of this suggestion was that detection had the connotation of 100% success, and the carriers felt that standard was unattainable. The FAA agreed and implemented the change. Later, in testimony to the 9-11 Commission, air carrier representatives were asked about their failure to detect the weapons used by the hijackers. Their response was that the rules only required them to deter weapons, not detect them.[41]

The air carriers were also successful in convincing the FAA to ignore the most forward-looking recommendations of the Baseline Working Group. As stated before, this group's work broke the FAA's long-standing history of reactive policy making, a move that was championed by many security advocates. The air carriers, however, argued that

---

[39] Johnstone, 21-26.

[40] George L. Priest, "Origins of Utility Regulation" *Journal of Law and Economics*, Vol. 36, no. 1, April 1993, 289-323.

[41] Johnstone, 27-28.

the absence of increasing domestic security incidents indicated that there was no reason to change the existing system. Their argument was based on the successful aviation safety program, in which policy changes are based on empirical evidence indicating areas in need of improvement. The FAA again backed down, and stopped pushing for its most comprehensive working group recommendations.[42]

Finally, the systematic reducing of fines for rule violations by the FAA provides a textbook example of regulatory capture. In her 9-11 commission testimony, former Department of Transportation Inspector General Mary Shiavo reported that her office had investigated the issue of fine reduction, and the results were troubling. In most cases, the investigators found that fines were reduced by approximately 90%, basically eliminating the penalty. Schiavo testified that "…you had a lot of tough talk…and then down the pike…when all the attention went away, the result was about ten cents on the dollar."[43]

4. Cumbersome Coordination between Federal Agencies

Perhaps the most discussed failure related to the 9-11 attacks is the failure of various federal agencies to coordinate on national security issues. Two areas that have drawn particular attention will be described here as examples. One relates to information sharing and the other to requesting assistance from other federal agencies.

On September 11, 2001, the FAA maintained its own no-fly list which was circulated to the air carriers via an FAA Security Directive. At the time of the attacks, this list contained just twelve names. Contrast this with the FBI terror watchlist, which contained over 40,000 names of known and suspected terrorists. Another list, the State Department's terror watchlist, was made available to the FAA prior to 9-11. This list, containing some 60,000 names, was reviewed by the FAA and declared "too difficult to use."[44]

---

[42] Johnstone, 37-43.

[43] Mary Schiavo, Inspector General, U.S. Department of Transportation, testimony to the National Commission on Terrorist Attacks Upon the United States, May 23, 2003, 86-87, http://www.9-11commission.gov/archive/hearing2/9-11Commission_Hearing_2003-05-23.pdf, accessed Nov. 8, 2007.

[44] *9-11 Commission Report*, 83-84.

The FAA and DoD had written procedures for responding to a domestic hijacking event. The DoD did not monitor domestic airspace, though it had the mission of defending U.S. airspace. At the time of the attacks, all DoD surveillance radars were on the coasts of the country, and watching outwards.[45] If the FAA required DoD assistance, a formal request had to be sent from the FAA Operations Center, through the National Military Command Center, to the Secretary of Defense. During the 9-11 attacks, numerous contacts were made between various FAA regional control centers and closely located military installations. None of these contacts were sufficient to gain a military response, per existing protocols. As noted in the earlier sections, though the FAA and DoD were communicating, information was slow to be passed, with most notifications occurring several layers down in the chain of command. The Secretary of Defense was only notified after Flight 77 had already struck the Pentagon.[46]

5. Ability to Close U.S. Airspace

One response action taken by the FAA during the 9-11 attacks has been widely praised. After the fourth hijacking was confirmed, the FAA issued a nationwide ground stop, which essentially closed the airspace over the continent U.S. This action had never been executed before, and by all accounts, was handled extremely well. Nearly 4,500 unplanned landings were accomplished in just over two and a half hours, all without incident.[47] At the time the order was issued, there was no way to be sure how many additional hijackings were in progressed or planned for that day. The ability for the FAA to clear the entire U.S. airspace in less than three hours shows one of the positive aspects of federal ownership and operation of a sector of our critical infrastructure.

---

[45] Larry Arnold, Major General, USAF, Commander of the U.S. Air Force's 1st Air Force, testimony to the National Commission on Terrorist Attacks Upon the United States, May 23, 2003, http://www.9-11commission.gov/archive/hearing2/9-11Commission_Hearing_2003-05-23.pdf, 28-29, accessed Nov. 8, 2007.

[46] Ibid., 19-22.

[47] See Griffith Testimony, note 21.

6. Analysis Summary

The federal response to the 9-11 hijackings showed both the positive and negative attributes of government's practical ownership in this sector. The FAA's dual mandate to both regulate and promote commercial aviation caused known security flaws to fall behind more visible priorities. These questionable priorities were also evident in the regulatory decisions made prior to the attacks, as costs and customer wait times won out over security. Despite these shortcomings, the FAA's ability to close the airspace over the U.S. in a matter of hours would have likely been lost if coordination among multiple decision makers would have been required. In total, the ownership role had more negative impacts than positive ones.

THIS PAGE INTENTIONALLY LEFT BLANK

III. FEDERAL GOVERNMENT AS A CUSTOMER — 2003 NORTHEAST BLACKOUT

A. BACKGROUND

In our modern society, few things if any impact our lives more than electricity. Most people take for granted that all the electricity they need will somehow be at their disposal, at just the time they need it. In the summer of 2003, millions of customers throughout the northeastern U.S. discovered just how precarious the electricity supply was as an untrimmed tree branch, accompanied by malfunctioning computer systems, caused one of the worst blackouts in U.S. history. The chapter analyzes how the circumstances surrounding this outage were enabled by the relationship between the federal government and the electricity industry.

1. Electricity 101

Electricity is ubiquitous. This never-ending stream of power is produced by what has been dubbed "the largest machine ever built."[48] The power grid comprises three distinct infrastructure components: generation, transmission, and distribution. Vast amounts of raw electricity are moved closer to the end customer via the high-voltage transmission system. Throughout the transmission system, substations are strategically placed to route power to local customers via the distribution system.[49]

The defining characteristic of the power grid is the level of interdependence among the grid components. Each generation, transmission, and distribution component is designed to handle a certain load. Suboptimal loads (either high or low) are disruptive to the grid, to the point of causing physical damage to the individual components. This interdependence requires a remarkable level of minute-by-minute monitoring and flow control. Generators must respond to demand changes while the transmission system

[48] Philip E. Auerswald, Lewis M. Branscomb, Todd M. LaPorte, Erwann O. Michel-Kerjan, eds., *Seeds of Disaster, Roots of Response: How Private Action Can Reduce Public Vulnerability*, Cambridge University Press, New York, NY, 2006, 164.

[49] Ibid., 194-197.

adjusts to varying system loads. Bulk power must be constantly rerouted around transmission outages. This coordination mechanism, spanning 250,000 miles of transmission lines and 65,000 substations, must function literally at the speed of light, making automated control systems absolutely essential.[50]

2. The Federal Government's Role in Overseeing the Grid[51]

The growth of the electricity industry supported the rapid industrialization of America in the early twentieth century. Power was often generated in or near urban industrial centers, minimizing the role of the transmission system. As environmental and safety concerns began to push power generation into less populated areas, the need for a robust transmission capability increased. Vertically integrated organizations dominated the industry for most of the twentieth century, providing all three components of the power grid. The Federal Power Commission, followed by its successor the Federal Energy Regulatory Commission, provided federal oversight of this industry, focusing mostly on prevention of price gouging.

Major blackouts in the 1960s spurred the Congress to propose legislation forcing stronger federal regulation of the power grid. In response, the industry formed the North American Electric Reliability Corporation (NERC), its charter being to develop and enforce operating standards on its members. This move convinced the Congress that additional federal regulation was not needed. NERC proceeded to develop standards which were voluntary for its members to follow; NERC had no legal authority to enforce them. This optional self-regulation was further complicated by the deregulation push of

[50] Auerswald, 198-201. The level of coordination required to support the grid cannot be overstated. Power production is dispatched to meet constantly fluctuating demand on an hourly basis, then fine-tuned throughout the hour. All of this happens across transmission areas covering multiple states.

[51] Stan Johnson, Manager of Situation Awareness and Infrastructure Security, North American Electric Reliability Corporation, interviewed by the author on 23 August, 2007. Unless specifically cited otherwise, all information in this section is adapted from this interview.

the 1980s, which resulted in the breakup of the vertically integrated grid operators. This resulted in even less control of a critical infrastructure which demands oversight by its highly interdependent design.[52]

NERC's mission expanded in the late 1990s to include critical infrastructure protection. NERC operates the electricity sector's Information Sharing and Analysis Center, a forum for crosstalk among the private sector power producers and between the sector and the federal government.[53] By supporting this voluntary self-regulation, the federal government in effect became a customer of the industry's infrastructure restoration processes.

B. ANATOMY OF A BLACKOUT [54]

1. Context of the 2003 Northeast Blackout

The subject blackout occurred in the largest of North America's power sector, the Eastern Interconnection. This sector encompasses the eastern two-thirds of the United States and portions of southeast Canada. Responsibility for grid reliability in the blackout area was shared by three regional reliability councils, under the oversight of NERC. Additionally, there were five control areas directly impacted by the blackout. Control area operators are directly responsible for the daily operations of the grid components within their areas.

NERC and its member organizations operate the power grid according to the "N-1 Criteria." This structure requires that the grid be able to remain stable during the worst single contingency for 30 minutes. During this 30-minute period, control area operators must restore the grid to its pre-contingency state or make adjustments to all components

---

[52] Additional information on the history of NERC can be obtained at its website, http://www.nerc.com, accessed Oct. 3, 2007.

[53] *National Infrastructure Protection Plan*, 51-69. The referenced section of the NIPP explains the various information sharing forums put in place by DSH. The Information Sharing and Analysis Center is the primary structure for private sector companies to share proprietary information on threats and in-place protection measures.

[54] U.S.-Canada Power System Outage Task Force, *Final Report on the August 14, 2003 Blackout in the United States and Canada: Causes and Recommendations*, North American Electric Reliability Corporation, Princeton, NJ, 2004, 5-12.

to prepare for the worst next contingency (the N-2 event). These preparations require both real-time awareness of grid components and detailed coordination with neighboring control areas.

2. Blackout Events and Impacts[55]

Customer demands for electricity on August 14, 2003 were high but well within the normal operating ranges of the power system. At approximately 10:00 am, grid operators in Ohio began experiencing glitches with their computer control systems. This limited the situational awareness of the grid status in Ohio, leaving controllers unaware of failures in key transmission lines in their sectors. These unknown outages became critical as the afternoon heat began to increase the demand for electricity. Ohio operators began to increase generation to meet the demand, and automatic systems kicked in to import power from neighboring control areas.

As additional power poured into Ohio, the transmission system continued to crumble. The status displays from the degraded monitoring systems left controllers unable to reconcile field reports of local outages and dangerous loading indicators from power generators. By approximately 4:00 pm, the high-voltage transmission system across the eastern interconnection had reached a critical state. Finally, the failure of a key line in eastern Ohio began an unstoppable cascading failure. Automatic equipment protection mechanisms began to kick in across the region, tripping transmission circuits and shutting down generators. Within 10 minutes the outage spread from Ohio to the East Coast, and north into Canada, affecting some 50 million people.

The August 2003 blackout goes down as one of the worst ever in North America. Cost estimates of the impact vary, with the generally accepted amount at $6 Billion.[56] The grid was restored for limited operations in 26 hours, with full restoration requiring 96

---

[55] *Final Report on the August 14, 2003 Blackout*, 23-93. This blackout was remarkable in its technical complexity. The following paragraphs provide a cursory description at best. Readers interested in the detailed explanations should consult the full report.

[56] Ibid., 1. Other estimates are summarized in the following: Electricity Consumers Resource Council, *The Economic Impacts of the August 2003 Blackout*, 2004, http://www.elcon.org/Documents/EconomicImpactsOfAugust2003Blackout.pdf, accessed Oct. 2, 2007.

hours. The following analysis will describe how the federal government's assuming the customer role affected the time necessary for restoration of power and the cost associated with this outage.

C. CASE ANALYSIS

1. Overall Analysis

The federal government's limited oversight role contributed to the duration and cost of the 2003 Blackout. NERC has cited four main causes of the outage: 1) failure of the Ohio reliability coordinator to plan enough reactive power for August 14; 2) loss of situational awareness on critical sections of the grid; 3) failure to manage vegetation growth in power line rights-of-way; and 4) failure of the regional reliability coordinators to provide real-time diagnostic support.[57] Though little could be done to speed recovery or lessen the financial impacts of the blackout once it occurred, it is clear that the scope of the blackout could have been reduced with stronger oversight at the federal level. Three specific issues will be discussed here: guideline development, compliance evaluation, and federal regulatory focus on issues other than reliability.

2. Guideline Development

As a customer, the federal government allowed the electricity industry to develop its own operational guidelines.[58] Some of these guidelines proved to be insufficient, either directly contributing to the blackout or allowing it to grow in scope. The following areas will covered specifically in this analysis: 1) lack of guidelines requiring validation of computerized control and monitoring systems; 2) lack of guidelines for operator training and certification; and 3) lack of guidelines for information sharing among reliability coordinators.

---

[57] *Final Report on the August 14, 2003 Blackout*, 18-19.

[58] Per the Johnson interview, NERC develops standards using American National Standards Institute processes. The standards are then reviewed by and voted on by the members of NERC. A full description of the process is available at http://www.nerc.com, accessed Oct. 2, 2007.

a. Guidelines Requiring Validation of Computerized Control and Monitoring Systems

The complexity and interconnectedness of the power grid combine to present a unique and complicated management challenge. Control area operators require sophisticated automated tools to provide real-time awareness of the grid's status and to assist with look-ahead planning for grid adjustments. The systems in place during the 2003 Blackout failed in both regards.

The Reliability Coordinator for Ohio repeatedly lost situational awareness of their control area on August 14. The monitoring and control system had been recently upgraded, and operators were continuing to find and diagnose system errors while using the system operationally. NERC's final investigative report states that the system provided outdated status information for several hours leading up to the blackout.[59] Additional errors were cited in the estimation tools used by other reliability organizations. The erroneous data produced by these estimation tools, themselves caused by poor system status information, prevented operators from making adjustments that could have limited the cascade of blackout conditions. While computer software glitches are unavoidable, allowing untested systems to be used in this demanding environment is risky management as best. Guidelines requiring documented validation of computer system testing and performance prior to implementation could have prevented one of the blackout's significant contributing factors. Other critical infrastructure sectors, such as finance, have adopted verification procedures for the communications systems used by their members.[60] These guidelines are part of the mandatory business continuity plans required in this sector.[61]

---

[59] *Final Report on the August 14, 2003 Blackout*, 45-50.

[60] Financial Services Sector Coordinating Council, *Financial Services Sector 2006 Annual Report*, https://www.fsscc.org/reports/2006/annual_report_2006.pdf, 128-131, Washington, DC, accessed Nov. 21, 2007.

[61] Lee Wrobel, "Legal Requirements for Disaster Recovery Planning: Common Facts and Misconceptions," InformIT, http://www.informit.com/articles/article.aspx?p=777896&rl=1, accessed Nov. 17, 2007.

b. Guidelines for Operator Training and Certification

In addition to these technical issues, NERC documented numerous instances where operators and technicians had not been trained on existing guidelines and procedures. Operators did not follow established procedures for updating neighboring control areas on existing contingency scenarios. Since control area operators do not have visibility into upstream or downstream areas, they require inputs from other operators regarding the status of their grid. In this case, existing guidelines were sufficient, but operators were not trained on them. The federal government could address this shortfall be requiring control area operators obtain certification on grid operation and restoration procedures.

c. Guidelines for Information Sharing Between Reliability Coordinators

Given the inextricable linkages between the various components of the power grid, it seems unacceptably risky that sharing operational status and planning information is left to the discretion of the control area operators. This restricted information flow is further complicated by the inability of neighboring control areas to get any visibility of the overall grid status electronically; operators are limited to observing status of their own sectors. Since planning systems in each sector depend on the ability to import power from neighboring sectors, the isolated character of the grid's management systems is self-defeating.

This lack of information sharing directly contributed to Cause #4 noted above. The reliability coordinator for Ohio was unable to bring their significant analysis capabilities to bear on the growing problems on the grid in their control area due to the lack of visibility of the grid's status. By the time each player in the affected grid sectors gathered the available and relevant information, the conditions for an unstoppable cascading outage were already present. Any actions taken at that point were too little, too late.

3. Compliance Evaluation

The previous section describes several instances in which existing industry-developed guidelines were insufficient to address the causes of the 2003 Blackout. Unfortunately, even if these guidelines were in place, NERC had neither the processes in place to verify compliance with them, nor the authority to enforce them. Two of the four cited causes of this blackout were direct violations of existing guidelines: 1) failure to plan for adequate reactive power to maintain the grid within N-1 standards; and 3) failure to follow guidelines for vegetation management in power line rights-of-way.

Both NERC and FERC seemed comfortable with the federal government's assumption of the customer role. Perhaps the 99.8% availability rate of the grid convinced both sides that more oversight was unnecessary. It is also clear that more heavy-handed regulation from the federal government was not politically enticing to DHS.[62] Unfortunately, the lax compliance regime that emerged from this relationship directly contributed to the 2003 Blackout.

4. Regulatory Focus on Issues Other Than Reliability

The final contributory effect of the government's customer role was the FERC's limited regulatory focus on infrastructure restoration and reliability. Keeping rates at a minimum was, and remains, FERC's overriding goal. The Commission's website states its core responsibility is "to guard the consumer from exploitation by non-competitive power companies."[63] When regulatory decisions were driven by this rate-conscious mindset, NERC had little chance of cajoling its members to impact their bottom lines with investments in reliability. Two of the blackout's main causes (poor operational planning and loss of situational awareness) reflected management decisions by the Ohio grid operator based on cost reduction, not reliability. Training operators to detect subtle anomalies in the grid and react in a manner timely enough to avert disaster is expensive. Additionally, fielding a critical control system without adequate testing and verification is

---

[62] *National Strategy to Secure Cyberspace*, 17.

[63] FERC website, http://www.ferc.gov/industries/electric/indus-act/competition.asp, accessed Oct. 11, 2007.

another cost-saving decision with disastrous results. In an environment where cost containment is the major focus, neither of these decisions is surprising.[64]

Beyond these direct impacts, rate restrictions have had other unintended consequences. First, the push to lower end-customer costs forces providers to buy bulk power from the lowest-cost producers. Often, these producers are not located in close proximity to the local power provider. This forces more power onto an already saturated transmission system. Additionally, as rate constraints tend to restrict investment, each provider's daily planning often depends on importing power from neighboring control areas to meet contingency demands. When the transmission system fails, as it did in 2003, importing power to meet demand is not possible, and even contributes to the cascading nature of this outage.[65]

5. Analysis Summary

The customer role assumed by the federal government in overseeing the reliability of the power grid has worked well. The industry has responded by developing an extensive set of operating guidelines, the results of which have been quite remarkable in terms of power availability. The events in August 2003 exposed the missing component of this relationship: a requirement for mandatory compliance with the operating guidelines. This lack of enforceability allowed the two direct causes of the blackout to exist, and resulted in the largest blackout in U.S. history.

---

[64] *Final Report on the August 14, 2003 Blackout*, 107. In this reference, NERC asserts that poor vegetation management has contributed to major major power outages. Together with note 65 and the overall tone of the NERC report, the author infers that cost-consciousness was a major factor in the decision making process.

[65] Ibid., 103-104. Table 7.1 in the NERC report summarizes a list of nine factors which present looming challenges to the U.S. power grid. Four of the nine issues are related to reduced operating margins on the high-voltage transmission systems, due both to increase load and reduced investment. NERC states specifically that companies are "less willing to make investments in transmission reliability that do not increase revenues."

THIS PAGE INTENTIONALLY LEFT BLANK

IV. FEDERAL GOVERNMENT AS A COORDINATOR — 2005 COMMUNICATIONS RESPONSE TO HURRICANE KATRINA

Hurricane Katrina was one of the most destructive natural disasters in the history of the United States. Literally every sector of the Gulf Coast Region's infrastructure was severely damaged; the telecommunications sector was especially hard hit. A thorough review of each sector's restoration activities would be impossible to do in a limited case study. This chapter will focus exclusively on the telecommunications infrastructure, the damage it sustained, and the role of federal government played in coordinating its restoration. Economic impacts and restoration timelines will be adjusted to reflect a similarly limited view of this disaster.

A. BACKGROUND

1. Commercial Telecommunications 101

The telecommunications backbone, along with the nation's power grid, comprises a set of underlying infrastructure that enables most of our modern culture and economy to function. The bundle of networks and equipment making up the backbone is often called cyberspace. A cursory understanding of cyberspace will allow the reader to appreciate how complex a management challenge it presents. Cyberspace is best understood by briefly examining its physical and logical characteristics.

The cyberspace backbone is physically constructed of high-capacity fiber optic cables, connected by the necessary switching equipment to facilitate accurate flow of data packets. The modern cyberspace backbone has become increasingly convergent, meaning that it carries data packets of many types, ranging from computer network traffic to voice telephone calls to television programming. More recently, technology advances have allowed wireless backbone segments to be implemented in areas where high-speed cabling is not available. While this convergent network is economically efficient, it also increases the likelihood that any significant disruption of the backbone will impact numerous if not all methods of electronic communications.

Customer access to the cyberspace backbone is provided by what the industry calls "the last mile." This connection is provided in a variety of ways, from high-speed cable, to Digital Subscriber Line (DSL), to regular telephone wiring, to wireless connections. In fact, convergence has reached the end user as well, with many homes receiving their telephone, computer network, and television access via a single connection. Clearly, both the backbone and customer access connections must be functional to allow these capabilities to be used as needed.

This extensive web of backbone and end user connectivity would be useless without the logical processes and protocols that allow packet transmission. As one might imagine, this transmission requires a high degree of standardization among the many companies that provide cyber services. The industry is mostly self-governed in this regard, with standards being determined by consensus among the largest service providers and user communities. Users hardly think twice about calling another person, sending an email, or browsing a website. Any of these activities likely involves many different service providers, all of which exchange packets of different types and get them to their proper destinations.[66]

2. The Federal Government's Role in Overseeing the Sector

Oversight of the telecommunications sector is divided between the Federal Communications Commission (FCC) and the Department of Homeland Security (DHS).[67] The FCC, as the primary regulatory agency for this sector, has a broad mission to oversee the day-to-day operations, with its responsibilities including "regulating interstate and international communications by radio, television, wire, satellite and cable."[68] For issues related to critical infrastructure protection and disaster response, the

[66] This description is based on the author's professional experience.

[67] *National Infrastructure Protection Plan*, 3.

[68] Federal Communications Commission website, http://www.fcc.gov/aboutus.html, accessed Nov. 19, 2007.

FCC has created the Public Safety and Homeland Security Bureau. This bureau consolidated functions which, at the time of Hurricane Katrina, were accomplished by various entities within the FCC.[69]

The FCC has realized that the complexities of modern telecommunications industry require cooperation between the major providers, as well as between the industry and the federal government. To facilitate this cooperation, the Commission chartered the Network Reliability and Interoperability Council (NRIC). NRIC was originally formed in 1992 to address a series of prolonged outages in the telephone switching infrastructure. Since that time, the FCC has repeatedly rechartered NRIC to address various issues such as the Year 2000 problem, and most recently critical infrastructure protection. NRIC comprises CEO-level representatives from some 35 communications providers, and forms focus groups to tackle each problem area referred to it by the FCC. The guidelines and best practices published by the NRIC are not mandatory and are not enforced by the FCC.[70]

The National Infrastructure Protection Plan gave DHS responsibility for the telecommunications sector with regard to critical infrastructure protection.[71] During a disaster, the FCC works within the overall federal response structure, in accordance with the National Response Plan. Cyberspace infrastructure issues requiring federal assistance are addressed through two separate channels during a disaster. The first of these channels involves national security communications. Any issues regarding critical federal government communications are addressed by the National Communications System through its National Coordinating Center for Telecommunications (NCC). The FCC provides direct support to the NCC. The FCC typically establishes the second coordination channel by placing personnel within the Joint Field Office directing the federal disaster response. Requests for FCC support dealing with local infrastructure

[69] Public Safety and Homeland Security Bureau, website, http://www.fcc.gov/pshs/, accessed Nov. 19, 2007.

[70] Network Reliability and Interoperability Council website, http://www.nric.org, accessed Nov. 19, 2007.

[71] *National Infrastructure Protection Plan*, 3.

restoration are addressed via this channel. Since many of the commercial providers support both national and local communications infrastructures, many of these requests are processed through the NCC as well.[72]

B. ANATOMY OF A TELECOMMUNICATIONS OUTAGE

1. Context of Hurricane Katrina's Telecommunications Impacts

As the previous section describes, federal oversight of the telecommunications sector is fragmented. The fragmentation is evident when reviewing the results of the various coordinating bodies involved in this sector. In short, the overwhelming focus of DHS oversight has been on improving cyber security within the sector,[73] whereas the FCC efforts have been aimed at building processes for resilience into the day-to-day operations of the commercial providers.[74] While the two-pronged approach does not preclude successful oversight, it does present a requirement for coordination at the federal level which was not in place during the response to Katrina. Many DHS initiatives had yet to be supported with the detailed planning necessary to implement them when Katrina struck.[75] It is against this backdrop of uncoordinated oversight that Hurricane Katrina and its aftermath unfolded.

---

[72] Kenneth P. Moran, Director of Office of Homeland Security, Federal Communications Commission, testimony to the Hearing on Hurricane Katrina and Communications Interoperability, U.S. Senate Committee on Commerce, Science, and Transportation, Sept. 29, 2005, 5-7.

[73] Government Accountability Office, *Internet Infrastructure: DHS Faces Challenges in Developing a Joint Public/Private Recovery Plan*, Government Accountability Office, Washington, DC, June 2006, 18-21.

[74] Mission statement of the Public Safety and Homeland Security Bureau, http://www.fcc.gov/pshs/, accessed Nov. 20, 2007.

[75] GAO, *DHS Faces Challenges in Developing a Joint Public/Private Recovery Plan*, 29-30.

2. Telecommunications Infrastructure Events and Impacts[76]

"Katrina" quietly entered the U.S. consciousness as Tropical Depression 12 on August 23, 2005. It was officially named "Tropical Storm Katrina" the following day, as it strengthened and moved toward the U.S. The federal government's disaster response machine also began to move on the August 24, with FEMA deploying its advance preparation unit, the Hurricane Liaison Team. FEMA also put its Gulf Coast Region on alert in case backup support was needed for the forecast Florida landfall. Katrina came ashore on Florida's eastern coast at approximately 6:30 pm local time.

Many hurricanes that cross southern Florida and enter the Gulf of Mexico make a second landfall along the Gulf Coast; Katrina followed this traditional path. The National Hurricane Center predicted on August 26 that Katrina would again make landfall, this time as a Category 4 storm. Both Mississippi and Louisiana declared states of emergency that day, which fully energized each state's disaster management organizations. FEMA continued its daily planning teleconferences, which had begun some two days earlier, to coordinate federal staging activities. August 27 saw the beginning of mandatory evacuations from the most dangerous sections of Louisiana and Mississippi; evacuation orders continued into the following day. FEMA continued to mobilize its management, logistics, and medical teams from the nearby regional centers. Late on August 27, President Bush issued federal emergency declarations for Mississippi, Alabama, and Louisiana, authorizing federal expenditures to help meet state requirements.

By late afternoon on August 28, Katrina's winds were beginning to affect evacuation operations, and shelters in the area were beginning to fill. Last minute increases to water and food stockpiles were made before rain and wind curtailed most preparatory operations. Katrina made landfall at 6:10 am on August 29 as a Category 3 storm. By noon that day, reports of levee failures throughout New Orleans began to reach officials. Within a day's time, 80% of the city was flooded.

---

[76] Katrina Lessons Learned Staff, *The Federal Response to Hurricane Katrina: Lessons Learned,* Office of the President of the United States, February 2006, 1-50. Most of this section is based on this report. Data from other sources will be specifically cited. The reader should also note that data specific to the timelines of telecommunications infrastructure failure and restoration is not readily available.

The overall impact of Katrina on the Gulf Coast was remarkable. It was the most destructive natural disaster in U.S. history, and the most deadly one since 1920. Isolating the impacts on the telecommunications sector is difficult, but some sector-specific information is available. The two largest commercial providers in the area, Sprint and BellSouth, reported their infrastructure repair costs would total between $600 and $800 million.[77] Some three million customers were without telephone service, with some 80% restored within 10 days of Katrina's landfall.[78] Some areas of New Orleans are still without full telecommunications services today.[79]

C. CASE ANALYSIS

1. Overall Analysis

The shortfalls in the federal response to Hurricane Katrina are well documented and have been discussed at length in many forums. As noted above, specific timelines for restoration activities for specific infrastructures are lacking. This does not, however, preclude the identification of some general positive and negative contributions of the coordination role assumed by the federal government in the telecommunications sector. This analysis will address the following areas: 1) coordination of regulatory waiver requests; and 2) coordination of restoration requirements.

2. Coordination of Regulation Waiver Requests

In addition to the technical complexities for successful infrastructure sharing described earlier, the FCC has numerous regulatory requirements governing access to the telecommunications backbone networks. To facilitate rapid restoration of infrastructure affected by Katrina, the FCC waived numerous regulatory requirements. According to the FCC's Director of Homeland Security, some 190 requests were received in the first

---

[77] Roseanne Gerin, "Telecoms Ride to the Rescue: Carriers Turn Out in Force to Aid Katrina Recovery Effort," *Washington Technology*, Vol. 20, No. 19, Sept. 2005, 1.

[78] GAO, *DHS Faces Challenges in Developing a Joint Public/Private Recovery Plan*, 26.

[79] Marlys Harris, "You Can't Go Home Again," *Money Magazine*, August 2007, http://money.cnn.com/2007/08/01/pf/neworleans_pellissier.moneymag/index.htm, accessed Nov. 21, 2007.

14 days of the restoration. The vast majority of the requests were approved within four hours, with none taking longer than 24 hours. These requests varied from applications for temporary radio frequencies to suspension of equal access requirements. Many of these requests, particularly those involving radio or satellite frequencies, required coordination with other customers to avoid interference.[80] For illustration, two requests will be detailed below.

FCC requirements basically require backbone providers to allow equal access to their networks to all other providers at fair rates. While these rates are not controlled by the FCC, providers may not use discriminatory pricing to give unfair advantage to a particular vendor, including its own subsidiaries which may provide local services in an area. BellSouth requested special authorization to re-route traffic from its subsidiary, BellSouth Long Distance, over the unaffected portions of its regional network. Normally, this would not have been allowed since it gives the subsidiary an unfair competitive advantage.[81]

Another familiar FCC regulation prohibits an activity known as slamming, where a local telephone provider switches a customer's long distance carrier without explicit permission from the customer. This normally subjects the customer to transfer fees and perhaps even higher charges. In many instances following Katrina, vendors requested relief from this requirement to facilitate restoration; the FCC readily approved these requests.[82]

These waivers positively affected the restoration in two ways. First, waivers for discriminatory access to backbone networks normally take months to adjudicate.[83] The speed with which the FCC responded shortened the restoration time by weeks.

---

[80] Moran, 5.

[81] Federal Communications Commission, "Joint Application by BellSouth Corporation, BellSouth Telecommunications, Inc., and BellSouth Long Distance, Inc., for Provision of In-Region, Inter-LATA Services in Georgia and Louisiana," Federal Communications Commission, Washington, DC, Sept. 13, 2005, 1-3.

[82] Moran, Appendix A.

[83] Ibid.

Additionally, allowing the use of existing networks saved the vendors the additional expense of installing more temporary networks to facilitate their restoration efforts.

3. Coordination of Restoration Requirements

The FCC also assumed responsibility for coordinating the requirement of telecommunications sector responders with other sectors. Two examples will show the positive impacts of this coordination on the restoration efforts. First, security became a major issue for all responders. As the conditions in New Orleans worsened, many workers came under attack while attempting to accomplish their work. Federal and local authorities began to provide security details for repair teams to enable their work to continue. The FCC coordinated the schedules of telecommunications repair teams with other sectors to maximize the efficient use of security assets.[84]

The FCC also served as a conduit of telecommunications requirements between federal and local officials. Service providers would apprise the FCC of the services they were capable of offering, and the FCC would present these capabilities to response coordinators. For example, post-landfall evacuations were struggling to gain traction due to the inability to broadcast pickup locations to the population. The FCC was able to put providers with portable broadcast systems in contact with local officials, as well as expedite any regulatory relief necessary for these broadcasts.[85]

As one might expect, there were instances where the coordination could have been better. Two examples will make this point clear. As the aforementioned security situation worsened, local and military officials began to restrict access to the damaged areas. Many officials were not accepting identification credentials produced by the telecommunications vendors as valid for access. This was further complicated by the inability of federal officials to let responders know what types of credentials would be acceptable.[86] In addition to access issues, coordination across the sector response teams

---

[84] Moran, 4-7.

[85] Ibid.

[86] *Report and Recommendations to the Federal Communications Commission*, Independent Panel Reviewing the Impact of Hurricane Katrina on Communications Networks, June 2006, 14-19.

was lacking in regards to supplies needed for restoration. For example, many telecommunications providers contracted for their own fuel deliveries to keep their backup generators operational. During the deliveries, fuel trucks were often diverted to higher-priority requirements, such as rescue vehicle fuel supplies. As generator fuel supplies ran short, communications disruptions would occur and further hamper relief efforts. This confusion over requirement prioritization tended to slow restoration and frustrated the participants on both sides.[87]

4. Analysis Summary

As these brief examples show, the role of coordinator in the telecommunications sectors was thoroughly tested in the response to Hurricane Katrina. There were successes, such as coordination of regulatory relief and repair schedule coordination across infrastructure sectors. There were, however, areas where coordination was lacking, particularly in repair supply delivery and in controlling access to the disaster areas. Overall, properly executed coordination had a positive impact on the restoration activities.

[87] *Report and Recommendations to the Federal Communications Commission*, Independent Panel Reviewing the Impact of Hurricane Katrina on Communications Networks, June 2006, 14-19.

THIS PAGE INTENTIONALLY LEFT BLANK

V. FEDERAL GOVERNMENT AS A REGULATOR — 2006 E. COLI OUTBREAK

A. BACKGROUND

In the summer of 2006, American's were given the rare occasion to question the safety of their food supply. Fresh spinach, grown in California, was linked to an outbreak of E. coli spread across the country. A joint state and federal investigation would soon reveal lapses on the part of growers and processors, and even on the part of the federal regulators charged with overseeing this vital sector of the U.S. economy.

1. Food Production 101

America has long been called the breadbasket of the world. Over the nearly three centuries of our nation's history, agriculture has grown from a means of family sustenance to a multibillion dollar per year industry. In Fiscal Year 2006, agriculture contributed some 1% of the nation's Gross Domestic Product. In addition to supporting domestic consumption, U.S. agricultural exports in FY 2006 were nearly $69 billion.[88] This critical infrastructure sector comprises a complex network of growers, harvesters, processors, retailers, and supporting trade organizations linking domestic and international consumers to farmers.

This case study deals only with the fresh produce segment of the food sector, which itself constitutes a rather complex structure making oversight and food safety challenging to say the least. In most regions, each player in the process (land owners, growers, harvesters and processors) are separate commercial entities. Most packaged products will likely contain produce from different growers within the same package. Safety of this critical food sector is managed via a process called Hazard Assessment and Critical Control Points (HACCP). Using this process, each entity in the flow assesses points at which hazards could endanger food safety. These hazard entry points are then

[88] U.S. Department of Agriculture, *Outlook for U.S. Agricultural Trade*, U.S. Department of Agriculture, Washington, DC, Aug. 2007, 1-4.

tightly managed with Critical Control Points, most of which entail manual inspection or preventive measures such as product washing, safe handling practices, or utensil sterilization.[89]

2. The Federal Government's Role in Overseeing the Sector

Responsibility for the food sector, from the homeland security perspective, is shared by the U.S. Department of Agriculture and the Department of Health and Human Services. The USDA monitors the meat, poultry, and egg sectors, while HHS oversees production of all other food products.[90] HHS implements a two-prong strategy to achieve a safe and reliable U.S. food sector. Preventing food-borne illnesses is obviously the preferred approach, and this is the primary mission of the Center for Food Safety and Applied Nutrition (CFSAN). Understanding that 100% prevention is not possible, HHS also maintains a significant outbreak response and investigation capabilities within the Centers for Disease Control and Prevention (CDC). Each of these strategic components is described in detail in the following paragraphs.

Preventing a food-born illness in the United States is a monumental task. In all, the CSFAN has oversight responsibility for 420,000 registered food establishments.[91] CFSAN tackles this problem with three main tools. First, CSFAN produces industry guidelines on food safety, covering the full landscape of the food sector, from growers to harvesters to processors, even consumers. Trace-back accountability is the one guideline that stands out as a key to food-born illness prevention. Meticulous record-keeping is required to ensure any contaminated product can be linked to its source. The second tool, food-related research, supports the first. CFSAN invests some $30 million per year in food safety research, mostly aimed at better prevention of food contamination during processing. Finally, the government relies on nearly 100 formal partnership agreements with various entities to implement its food safety inspection programs. These partners

---

[89] California Emergency Response Team, *Investigation of an Escherichia coli O157:H7 Outbreak Associated with Dole Pre-Packaged Spinach*, Sacramento, CA, March 2007, 4-16.

[90] *The National Infrastructure Protection Plan*, 3.

[91] American Society for Microbiology Position Statement on FY2007 FDA Budget Proposal, http://www.asm.org/Policy/index.asp?bid=41959, accessed Oct. 25, 2007.

include state and local governments as well as industry associations and third party inspectors, all of which agree to use FDA guidelines to inspect commercial food entities under their purview. It should be noted that, while authorized, these third party reviews are not synonymous with, or a legal replacement for, an FDA inspection.[92]

Responding to and investigating outbreaks of food-born illnesses are similarly daunting tasks. The basic process involves identifying cases with confirmed presence of a known pathogen, then establishing the carrier vehicle for that pathogen. CDC publishes these virus "fingerprints" electronically across the country through a database called PulseNet. Given that food-born illnesses share symptoms with many normal maladies, there are often delays in confirmation of outbreaks as food related. OutbreakNet is the CDC-sponsored network of health professionals who investigate food-born illnesses.[93] This ability to uniquely identify the virus and isolate its carrier vehicle, coupled with the CFSAN's focus on trace-back accountability, constitutes the most critical federal capability for responding to any food-born outbreak.

B. ANATOMY OF A FOOD-BORN ILLNESS OUTBREAK

1. Context of the 2006 E. Coli Outbreak

California produces nearly 75% of the leafy green vegetables consumed in the U.S.[94] This virtual monopoly brings with it, however, much of the responsibility for the checkered history of food safety regarding these fresh vegetables. In the eleven years leading up to the 2006 spinach scare, there had been nine E. coli outbreaks related to California-grown vegetables. Most efforts to address this string of outbreaks were industry-led. In 2005, the FDA had warned state officials and industry leaders that

---

[92] "What Third Party Inspections Mean to You," http://www.naturalproductsinsider.com/articles/470/470_461cert.html, accessed Oct. 25, 2007.

[93] Centers for Disease Control and Prevention, "Food Outbreak Detection and Surveillance," available at http://www.cdc.gov/foodborneoutbreaks, accessed Oct. 25, 2007, 1-18.

[94] CBS News, "Salad Growers In a Spin Over E-Coli," http://www.cbsnews.com/stories/2007/09/13/health/main3257421.htm, accessed Oct. 22, 2007.

federal patience with local efforts was wearing thin. A second warning letter made the federal opinion very clear: "FDA is investigating regulatory options and will consider enforcement actions against firms and farms that grow, pack, or process fresh lettuce and leafy greens under insanitary [sic] conditions."[95]

After several years of planning, the California Food Emergency Response Team (CalFERT) was formed in 2005. This partnership between federal, state, and industry players provides the investigative response to any food-born illness outbreak. Most routine inspections of California growers are state-level reviews of handling process documentation. Some growers and processors use third-party evaluators to provide objective oversight of their internal operations. Despite these safety mechanisms, an investigation by CalFERT showed that many of the FDA's repeated warnings regarding food safety had not been heeded.[96]

2. Outbreak Events and Impacts

The first official notification to the CDC of a suspected E. coli outbreak was made on September 8, 2006. Wisconsin public health officials reported a cluster of cases, and had identified the strain of E. coli as O157:H7. These results were posted to PulseNet, and by September 12, two additional states had confirmed the presence of the same strain. Based on further research and patient interviews, officials in Wisconsin and Oregon notified the CDC on September 13 that they considered fresh spinach to be the likely carrier in this outbreak. The following day, the FDA advised consumers nationwide to avoid bagged fresh spinach. On September 15, the largest spinach

[95] U.S. Food and Drug Administration, "Letter to California Firms that Grow, Pack, Process, or Ship Fresh and Fresh-cut Lettuce," November, 2004, http://www.cfsan.fda/gov/~dms/prodltr2.html, accessed Oct. 19, 2007, 3.

[96] CalFERT, *Investigation of an Escherichia coli O157:H7 Outbreak Associated with Dole Pre-Packaged Spinach*, 3-4.

processor in California announced a voluntary recall of all bagged spinach products. One week later, FDA officials announced that the contamination had been isolated to three counties in California's Central Coast Region.[97]

CalFERT began its investigation on September 13. Inspectors arrived at the suspected facility on September 15 and immediately began to review company documentation for product traceback information. Affected lot numbers were identified on September 21, highlighting a batch of fresh-cut spinach harvested on August 14. Growers and harvesters associated with the suspect lot number were confirmed by September 24. Multiple environmental samples were collected from four suspect farms, and the outbreak strain was identified in one of the four locations.[98]

All told, the 2006 E. coli outbreak resulted in 203 confirmed infections, with over half (103) requiring hospitalization, and 3 deaths.[99] Itemized cost estimates from this outbreak are difficult to obtain, but most estimates place the economic impact at approximately $100 million.[100] The spinach sector operated in a degraded state for 30 days. Full operation of the sector was restored after 38 days.[101] The following analysis will describe how the federal government's regulator role affected the duration and the cost associated with this outbreak.

---

[97] U.S. Centers for Disease Control and Prevention, "Ongoing Multistate Outbreak of Escherichia coli serotype O157:H7 Infections Associated with Consumption of Fresh Spinach," Sep 26, 2006 Press Release, http://www.cdc.gov/mmwr/preview/mmwrhtml/mm55d926a1.htm, accessed Oct. 21, 2007.

[98] *Investigation of an Escherichia coli O157:H7 Outbreak Associated with Dole Pre-Packaged Spinach*, 17-48.

[99] Ibid., 4.

[100] Estimates of the costs range from $50M - $200M. None of the published estimates account for the costs of the investigation. For estimate details, see the following: Karen Klonsky "E. Coli in Spinach, Foodborne Illnesses, and Expectations about Food Saftey," *Agriculture and Resource Update*, Vol. 2, No. 2, Nov/Dec 2006, 1-4; Fox News, "E. Coli Outbreak Hurts Spinach Farming Industry, Restaurants," http://www.foxnews.com/story/0,2933,215257,00.htm, accessed Oct. 22, 2007; "Expanded research to target E. coli outbreaks," http://calag.ucop.edu/0701JFM/resup01.html, accessed Oct. 22, 2007.

[101] The judgment of the author was used to determine the length of this disruption. Using the CalFERT final report chronology, the period of the degraded operations was determined to be the period of time the sector could have been generating contaminated spinach. Full operations were deemed possible once the traceback accountability review had isolated the source of the contaminated spinach.

C. CASE ANALYSIS

1. Overall Analysis

CalFERT's thorough investigation identified the outbreak strain of E. coli O157:H7 at one of the four implicated fields. However, CalFERT investigators were unable to definitively determine how the spinach from that field became contaminated. Several possible methods of contamination were given, including the close proximity of fecal matter from grazing livestock and wildlife; contaminated irrigation water; and the use of animal manure as fertilizer. Environmental samples from the processing locations were negative for the outbreak strain, eliminating the possibility of post-harvest contamination. Once the outbreak was underway, the public health response was adequate, though on the upper end of timelines given in CDC reporting guidelines. The following analysis will discuss areas in both prevention and response where the government's regulator role had an impact on the duration and cost of this outbreak. Specific problems included 1) lax guidance from the FDA; 2) weaknesses in the FDA inspection program; 3) cumbersome record-keeping for traceback accountability; and 4) inconsistent reporting from state and local entities to the CDC.

2. Factors Contributing to Failed Prevention

a. Lax Guidance From the FDA

As a regulator of the food industry, the FDA provides a significant volume of guidance to the industry, covering every facet of the food production process from field operations to retail handling and storage. This guidance was lacking or unclear in several areas directly related to this outbreak. Consider the following quote from the FDA's *Guide to Minimize Microbial Food Safety Hazards of Fresh-Cut Fruits and Vegetables*:

> In general, anything that comes in contact with fresh produce has the potential to contaminate it. Fresh produce may become contaminated at any point along the farm-to-table continuum. The major source of microbial contamination of fresh produce is direct or indirect contact with

> animal or human feces. Once [it] has been contaminated, removing or killing the microbial pathogens is very difficult. Prevention of microbial contamination at all steps of the farm-to-table continuum is preferable to treatment to eliminate contamination after is has occurred.[102]

The guidance provided throughout the document either conflicts with or minimizes the importance of this prevention focus. First, despite championing HACCP as a proven "prevention-based food safety system," the FDA allows implementation of HACCP to remain optional for fresh-cut vegetable producers.[103] Further, generic guidance is given relating to prevention of animal feces contact with plants in the field. Growers are advised to "maximize the time" between application of manure-based fertilizers and planting, but no timeframe is given. Farmers are also encouraged to "consider sound measures" to keep waste from grazing cattle and other animals from entering fields during growing seasons; no source of these sound practices is given.[104] Both of these animal-related sources of contamination were cited as likely causes of this outbreak, yet neither is sufficiently addressed in FDA guidance.

b. Weaknesses in the FDA Inspection Program

The large and diverse food sector presents a challenging oversight problem to the FDA. Despite calls for increased formal inspections, the FDA inspects food producers just once every 3.9 years. This paucity of oversight is made worse by the fact that entities that fail inspections are not subject to fines or banishment from further food production.[105] The FDA attempts to address this inability to provide timely oversight by encouraging producers to use third party evaluations to check their internal

---

[102] Center for Food Safety and Applied Nutrition, *Guide to Minimize Microbial Food Safety Hazards of Fresh-Cut Fruits and Vegetables: Draft Final Guidance*, U.S. Food and Drug Administration, College Park, MD, 2007, 6.

[103] Ibid., 5.

[104] Ibid., 27.

[105] CBS News, "Salad Growers In a Spin Over E-Coli," http://www.cbsnews.com/stories/2007/09/13/health/main3257421.htm, accessed Oct. 22, 2007.

processes. These evaluators use FDA guidelines, and even receive FDA training, but their findings are not recognized as valid insofar as reducing the need for formal FDA visits.

3. Factors Contributing to Slow Outbreak Response[106]

a. Cumbersome Record Keeping for Traceback Accountability

A linchpin of the outbreak investigation process is the ability to trace suspect produce back to the source of origin. In this case, identification of spinach as the likely carrier occurred on September 13, 2006. Lot codes printed on the packaging allowed investigators to quickly focus on one processing facility in California. However, tracing the source of the spinach processed in the suspect lot number was difficult. The facility in question uses manual record keeping to record all process flow information, such as receipt of produce from the field, product grading, processing equipment testing, as so on. It took CalFERT investigators six additional days to trace the lot number to the fields of origin. Automated record keeping would likely have shortened this research time significantly. Local studies have shown that some processors have resisted efforts urging them to automate record keeping for traceback and other accountability information, mostly due to cost concerns. This same study noted that those processors with automated record keeping systems completed traceback queries within an hour of the request.[107]

b. Inconsistent Reporting from State and Local Entities to the CDC

According to the CDC timeline for this outbreak, the earliest illness caused by the outbreak strain was diagnosed on August 19, 2006. This case was

[106] It should be noted that a 4-9 day lag time always occurs at the beginning of any E. coli outbreak investigation. The incubation period of the pathogen is 3-4 days. Further, the CDC also estimates that those impacted by the illness often delay seeking treatment by up to 5 days, if they seek treatment at all. Details on the reporting timeline can be found at http://www.cdc.gov/ecoli/reportingtimeline.htm, accessed Oct. 20, 2007.

[107] Gregory A. Baker, Ellen Farmer, and Ron Maysenhalder, *Reforming the Fresh Produce Food Safety System*, Food and Agribusiness Institute, Santa Clara University, San Jose, CA, 2006, 2-5.

discovered later in the investigation, as the first reported cluster of cases was announced on September 8. This 3-week window is indicative of the reporting dilemma faced by CDC. As mentioned earlier, patient evaluation is accomplished in local health facilities. When illnesses are confirmed as being caused by pathogens on the CDC watch list, they are reported via PulseNet. Laboratory procedures and reporting protocols differ from location to location, so the timeliness of reporting can vary greatly. Reducing this variance in reporting could make a significant difference the overall time needed to isolate the source of an outbreak.

4. Analysis Summary

As the CalFERT investigation showed, the 2006 E. coli outbreak was not a surprise occurrence in California. The state had a long history of outbreaks, especially ones associated with leafy green vegetables. The investigation also showed that the FDA's inspection program had grown ineffective, with too much time between inspections and an over-reliance on industry self-inspection. The state's growers' implementation of manual traceback accounting further delayed the isolation of suspect fields. In response, growers have formed an industry association to develop more stringent guidelines, although these guidelines will not be mandatory. As Chapter III of this thesis shows, this approach does not ensure success.

THIS PAGE INTENTIONALLY LEFT BLANK

VI. CONCLUSIONS AND RECOMMENDATIONS

A. SUMMARY OF CASE STUDY VARIABLES

The goal of this thesis was to examine the impact of the various oversight roles assumed by the federal government on the restoration of different critical infrastructure sectors. Specifically, each case was analyzed based on the economic impact of the downtime, time required to reach initial operating capability (IOC), and time required to restore full operating capability (FOC). Table 1 provides a summary of the data from each case study. The direct impact of the government role on each of these variables will be discussed in the following section.

Case Study Incident (Sector)	Government Role	Economic Impact	Time to reach IOC	Time to reach FOC
2001 Terrorist Attacks (Aviation)	Owner	$1.4 billion	4 Days	26 Days
2003 Northeast Blackout (Electricity)	Customer	$6 billion	1 Day	4 Days
2005 Hurricane Katrina (Telecommunications)	Coordinator	$0.7 billion	10 Days	Ongoing
2006 E. coli Outbreak (Food)	Regulator	$0.1 billion	---	30 Days

Table 1. Summary of Case Study Variables

B. CONCLUSIONS ON THE IMPACT OF THE GOVERNMENT ROLE

1. Impact of Government Role on Cost

Based on details of the cases, *the role assumed by the federal government had no direct impact on the costs associated with each disruption*. The disparity in cost across the cases is the result of variations in the nature of the infrastructures involved. For example, the loss of electricity affects virtually everyone in the impacted areas in a variety of ways from food spoilage to lost wages or productivity to actual repair costs. An aviation disruption, however, affects a much smaller segment of the population and the economy of the nation. The nature of the disruption also affected costs. The infrastructure costs associated with Hurricane Katrina were enormous, due mainly to the overwhelming physical destruction caused by the storm's landfall and subsequent flooding. The other cases saw limited physical impacts to the actual infrastructures, so the costs were mainly limited to lost wages and productivity.

2. Impact of Government Role on Disruption Duration

In three of the four cases, the government role had direct impacts on the duration of the disruption. In the aviation case, the owner role had an overall negative impact on the duration. The FAA's dual mandate prevented its proper focus on domestic hijacking response measures, despite the fact the all of these response activities were within the purview of the federal government. This lack of focus extended the time necessary to confirm the hijackings and to formulate a response. These negative impacts were mitigated somewhat by the ability of the government to mandate interim security measures to facilitate the rapid resumption of air travel. *The overall impact of the owner role was a reduction of the time necessary to achieve the restoration of IOC and FOC in the aviation sector.*

The coordinator role had a similarly mixed impact on telecommunications restoration. On the positive side, the FCC's rapid coordination of regulatory waivers shortened the duration of the outage. Conversely, the problematic implementation of access credential programs and poor prioritization of material requirements had negative

effects on restoration efforts. *The overall impact of the coordinator role in the telecommunications sector was positive, reducing the time for both IOC and FOC restoration.*

The regulator role had a mostly negative impact on restoration of the food sector. This negative impact was clear in two areas. First, the delayed reporting between the local hospitals and laboratories and the CDC slowed the identification of the outbreak strain of E. coli. Further, the FDA's acceptance of and reliance upon manual traceback accounting records also extended the duration of the disruption by delaying the isolation of suspect fields. This negative impact is not inherent in the regulator role, but specifically related to the FDA's current structure. The GAO has pointed out that the FDA lacks statutory recall authority for food, though it has such authority for pharmaceuticals.[108] This reliance on voluntary recalls, coupled with the paltry inspection rate discussed in Chapter IV, further hampered the FDA's effectiveness in this sector.

C. OTHER CONSIDERATIONS/OBSERVATIONS

1. An Ounce of Prevention Really is Worth a Pound of Cure

While prevention was not one of the case variables measured in this study, it quickly emerged as a factor in three of the four cases. The Northeast Blackout was initiated by ineffective management of vegetation along high-voltage lines, despite the existence of clear prevention measures in NERC guidelines. The E. coli outbreak might have thwarted with stronger enforcement of the FDA's proven detection methods. Even the most infamous of the cases, the 9-11 attacks, was precipitated by a failure to properly screen passengers for proscribed items. The world would be a different place today if these achievable prevention methods had been effectively employed.

[108] Government Accountability Office, *Food Safety: USDA and FDA Need to Better Ensure Prompt and Complete Recalls of Potentially Unsafe Foods*, Government Accountability Office, Washington, DC, 2004, 2-5.

2. Let's Not Relearn the Lessons of the Past

As described in Chapter III of this thesis, the electricity sector learned a clear lesson that voluntary compliance enforcement does not work in a highly competitive industry. The government responded to this lesson by making all NERC reliability guidelines mandatory in the Energy Policy Act of 2005.[109] Unfortunately, other sectors have not learned from this. The FDA is allowing the food sector to respond to the most recent E. coli outbreak with voluntary, industry-developed guidelines. DHS and the FCC are following a similar path of allowing the telecommunications industry develop its own protection standards for voluntary compliance. A quick study of the power sector would show that a more rigorous approach is needed.

D. RECOMMENDATIONS FOR FUTURE STUDY

This study has highlighted three areas relevant to critical infrastructure protection which warrant further study. First, in assigning sector specific agencies to oversee the various infrastructure sectors, DHS has in some cases chosen the industry regulators while assigning other sectors to less directly related agencies. NERC has asserted that market and reliability decisions cannot be effectively made separately.[110] Testing this statement, in light of the oversight assignments made be DHS, would be beneficial. A related study would be to examine whether the weaknesses in the roles displayed in these cases are inherent in the role, or more related to the particular disruption. Finally, another interesting and useful study would be to examine whether a structure similar to NERC would applicable in the telecommunications sector. The two sectors are similar in the level of industry cooperation and coordination required, so attempting to apply the NERC model to telecommunications might prove worthwhile.

---

[109] Federal Energy Regulatory Commission, *Energy Policy Act of 2005 Fact Sheet*, U.S. Department of Energy, Washington, DC, 3-4.

[110] *Final Report on the August 14, 2003 Blackout in the United States and Canada: Causes and Recommendations,* 104.

LIST OF REFERENCES

Akintoye, Akintola, Matthias Beck, and Cliff Hardcastle, eds., *Public-Private Partnerships: Managing Risks and Opportunities*, Blackwell Publishing, Malden, MA, 2003.

Anonymous, "Public-Private Partnership Seen as Vital to Cybersecurity," *Telecommunications Reports*, Vol. 71, No. 19, October 1, 2005.

Anonymous, "U.S. Policy regarding Internet Governance", *The American Journal of International Law*, Vol. 99, No. 1, January 2005.

Arnone, Michael, "A Work In Progress," *Federal Computer Week*, August 28, 2006.

Auerswald, Philip E., Lewis M. Branscomb, Todd M. LaPorte, Erwann O. Michel-Kerjan, eds., *Seeds of Disaster, Roots of Response: How Private Action Can Reduce Public Vulnerability*, Cambridge University Press, New York, NY, 2006.

Ayres, Ian and John Braithwaite, "Partial-Industry Regulation: A Monopsony Standard for Consumer Protection," *California Law Review*, Vol. 80, No. 1, January 1992.

Baker, Gregory A., Ellen Farmer, and Ron Maysenhalder, *Reforming the Fresh Produce Food Safety System*, Food and Agribusiness Institute, Santa Clara University, San Jose, CA, 2006.

Bauer, Johannes M., Laurence Caby, and Charles Steinfield, eds., *Telecommunications in Transition: Policies, Services and Technologies in the European Community*, Sage Publications, Thousand Oaks, CA, 1994.

Birkland, Thomas A., *Lessons of Disaster: Policy Change after Catastrophic Events*, Georgetown University Press, Washington, DC, 2006

Brock, Gerald W., *Telecommunication Policy for the Information Age: From Monopoly to Competition*, Harvard University Press, Cambridge, MA, 1994.

Bureau of Economic Analysis, "Gross Domestic Product by Year," U.S. Department of Commerce, http://www.bea.gov/national/index.htm#gdp, accessed November 25, 2007.

California Emergency Response Team, *Investigation of an Escherichia coli O157:H7 Outbreak Associated with Dole Pre-Packaged Spinach*, Sacramento, CA, March 2007.

Center for Food Safety and Applied Nutrition, *Guide to Minimize Microbial Food Safety Hazards of Fresh-Cut Fruits and Vegetables: Draft Final Guidance*, U.S. Food and Drug Administration, College Park, MD, 2007.

Crandall, Robert W., *Competition and Chaos: US Telecommunications since the 1996 Telecom Act,* Brookings Institution Press, Washington, DC, 2005.

Crandall, Robert W. and Kenneth Flamm, eds., *Changing the Rules: Technological Change, International Competition and Regulation in Communications,* The Brookings Institute, Washington, DC, 1989.

Congressional Research Service, *Homeland Security: Banking and Financial Infrastructure Continuity,* Congressional Research Service, Washington, DC, March 2005.

Department of Homeland Security, *The National Infrastructure Protection Plan,* Department of Homeland Security, Washington, DC, 2006.

Department of Homeland Security, *The National Strategy to Secure Cyberspace,* Department of Homeland Security, Washington, DC, 2003.

Department of Labor, Occupational Labor Statistics (May 2005), Bureau of Labor Statistics, http://www.bls.gov/oes/home.htm, accessed April 11, 2007.

Federal Bureau of Investigation, *Terrorism 2000-2001,* U.S. Department of Justice, Washington, DC, 2002.

Federal Energy Regulatory Commission, *Energy Policy Act of 2005 Fact Sheet*, U.S. Department of Energy, Washington DC, 2005.

The Federal Response to Hurricane Katrina: Lessons Learned, Katrina Lessons Learned Staff, Office of the President of the United States, February 2006.

Financial Services Sector Coordinating Council, *Financial Services Sector 2006 Annual Report*, https://www.fsscc.org/reports/2006/annual_report_2006.pdf, accessed November 21, 2007.

Foldvary, Fred E. and Daniel B. Klein, eds, *The Half-Life of Policy Rationales: How New Technology Affects Old Policy Issues,* New York University Press, New York, NY, 2003.

Gerin, Roseanne, "Telecoms Ride to the Rescue: Carriers Turn Out in Force to Aid Katrina Recovery Effort," *Washington Technology,* Vol. 20, No. 19, September 2005.

Government Accountability Office, *Food Safety: USDA and FDA Need to Better Ensure Prompt and Complete Recalls of Potentially Unsafe Foods*, Government Accountability Office, Washington, DC, 2004.

Government Accountability Office, *Internet Infrastructure: DHS Faces Challenges in Developing a Joint Public/Private Recovery Plan*, Government Accountability Office, Washington, DC, 2006.

Government Accountability Office, *Critical Infrastructure Protection*, Government Accountability Office, Washington, DC, 2002.

Government Accountability Office, *Critical Infrastructure Protection*, Government Accountability Office, Washington, DC, 2007.

Grimsey, Darrin and Mervyn K. Lewis, *Public-Private Partnerships: The Worldwide Revolution in Infrastructure Provision and Project Finance*, Edward Elgar Publishing, Northampton, MA, 2004

Harris, Marlys, "You Can't Go Home Again," *Money Magazine*, August 2007, available online at http://money.cnn.com/2007/08/01/pf/neworleans_pellissier.moneymag/index.htm, accessed November 21, 2007.

Heinrich, Carolyn J. and Larrence E. Lynn, Jr., eds., *Governence and Performance: New Perspectives.*, Georgetown University Press, Washington, DC, 2000.

Hills, Jill, *Deregulating Telecom: Competition and Control in the United States, Japan, and Britain*, Quorum Books, Westport, CT, 1986.

Hodge, Graeme A., *The Challenge of Public-Private Sector Partnerships: Learning from International Experience*, Edward Elgar Publishing, Northampton, MA, 2005.

Horwitz, Robert Britt, *Irony of Regulatory Reform: The Deregulation of American Telecommunications*, Oxford University Press, New York, NY, 1991.

Johnstone, R. William, *9/11 and the Future of Transportation Security*, Praeger Security International, Westport, CT, 2006.

Klingler, Richard, *The New Information Industry: Regulatory Challenges and the First Amendment*, Brookings Institutions Press, Washington, DC, 1996.

Klonsky, Karen, "E. Coli in Spinach, Foodborne Illnesses, and Expectations about Food Saftey," *Agriculture and Resource Update*, Vol. 2, No. 2, Nov/Dec 2006.

Makinen, Gail, *The Economic Effects of 9/11: A Retrospective Assessment*, Congressional Research Service, Washington, DC, 2002.

McEntire, David A., *Disaster Response and Recovery: Strategies and Tactics for Resilience*, John Wiley and Sons, Inc., Hoboken, NJ, 2007.

Metropolitan Washington Airports Authority, *History of Ronald Reagan National Airport*, http://www.mwaa.com/_/File/_/history_DCA.pdf, accessed November 19, 2007.

National Commission on the Terrorist Attacks Upon the United States, *Staff Statement #4*, National Commission on the Terror Attacks upon the United States, Washington, DC, http://www.9-11commission.gov/staff_statements/staff_statement_4.pdf, accessed November 6, 2007.

National Commission on the Terrorist Attacks Upon the United States, *Testimony of Mr. Jeff Griffith, Deputy Director of Air Traffic at the Federal Aviation Administration*, National Commission On the Terrorist Attacks Upon the United States, Washington, DC, June 2004, http://www.9-11commission.gov/hearings/hearing12/griffith_statement.pdf, accessed November 6, 2007.

National Commission on the Terrorist Attacks Upon the United States, *Testimony of Ms. Mary Schiavo, Inspector General, U.S. Department of Transportation*, National Commission on Terrorist Attacks Upon the United States, Washington, DC, May 2003, http://www.9-11commission.gov/archive/hearing2/9-11Commission_Hearing_2003-05-23.pdf, accessed November 6, 2007.

National Commission on the Terrorist Attacks Upon the United States, *Testimony of Mr. Mike Canavan, Associate Administrator for Civil Aviation Security, Federal Aviation Administration*, National Commission on Terrorist Attacks Upon the United States, Washington, DC, May 2003, http://www.9-11commission.gov/archive/hearing2/9-11Commission_Hearing_2003-05-23.pdf, accessed November 6, 2007.

National Commission on the Terrorist Attacks Upon the United States, *Testimony of Major General Larry Arnold, Commander of the U.S. Air Force's 1st Air Force*, National Commission on Terrorist Attacks Upon the United States, Washington, DC, May 2003, http://www.9-11commission.gov/archive/hearing2/9-11Commission_Hearing_2003-05-23.pdf, accessed November 6, 2007.

Priest, George L., "Origins of Utility Regulation," *Journal of Law and Economics*, Vol. 36, No. 1, April 1993.

Report and Recommendations to the Federal Communications Commission, Independent Panel Reviewing the Impact of Hurricane Katrina on Communications Networks, June, 2006.

Rothkopf, David J., "Business Versus Terror," *Foreign Policy*, May-June 2002.

Snow, Marcellus S. *Marketplace for Telecommunications: Regulation and Deregulation in Industrialized Democracies*, Longman Incorporated, New York, NY, 1986.

Stanton, Thomas H., editor, *Meeting the Challenge of 9/11: Blueprints for More Effective Government*, M.E. Sharpe, Armonk, NY, 2006.

The Unpredictable Certainty: Information Infrastructure Through 2000, National Academy Press, Washington, DC, 1996.

U.S.-Canada Power System Outage Task Force, *Final Report on the August 14, 2003 Blackout in the United States and Canada: Causes and Recommendations*, North American Electric Reliability Corporation, Princeton, NJ, 2004.

U.S. Census Bureau, *Measuring the Electronic Economy*, 2004, http://www.census.gov/econ/www/ebusiness614.htm, accessed April 11, 2007.

U.S. Centers for Disease Control and Prevention, "Ongoing Multistate Outbreak of Escherichia coli serotype O157:H7 Infections Associated with Consumption of Fresh Spinach," September 26, 2006, http://www.cdc.gov/mmwr/preview/mmwrhtml/mm55d926a1.htm, accessed October 21, 2007.

U.S. Congress, House Committee on Energy and Commerce, Subcommittee on Telecommunications and the Internet, *Cybersecurity Protection, testimony of Mr. George S. Forseman*, Washington, DC, September 13, 2006.

U.S. Congress, House Committee on Energy and Commerce, Subcommittee on Telecommunications and the Internet, *Cybersecurity Protection, Testimony of Mr. Vincent Weafer*, Washington, DC, September 13, 2006.

U.S. Congress, House Committee on Homeland Security, Subcommittee on Economic Security, Telecommunications, and Cybersecurity, *Future of DHS Cyber and Telecommunications Security, Testimony of Mr. David M. Barron*, Washington, DC, September 13, 2006.

U.S. Congress, House Committee on Homeland Security, Subcommittee on Economic Security, Telecommunications, and Cybersecurity, *Future of DHS Cyber and Telecommunications Security, Testimony of Mr. Paul B. Kurtz*, Washington, DC, September 13, 2006.

U.S. Congress, Senate Committee on Commerce, Science, and Transportation, *Testimony of Kenneth P. Moran, Director of Office of Homeland Security, Federal Communications Commission,* Washington, DC, September 29, 2005.

U.S. Food and Drug Administration, "Letter to California Firms that Grow, Pack, Process, or Ship Fresh and Fresh-cut Lettuce," November 2004, http://www.cfsan.fda/gov/~dms/prodltr2.html, accessed October 19, 2007.

Wilks, Stephen and Maurice Wright, eds., *Comparative Government-Industry Relations: Western Europe, the United States, and Japan,* Oxford University Press, New York, NY. 1987.

Willis, Jonathan L., "What Impact will E-Commerce Have on the US Economy?" U.S. Federal Reserve Bank of Kansas City, 2002, http://www.kansascityfed.org/Publicat/econrev/Pdf/2q04will.pdf, accessed April 11, 2007.

Wrobel, Lee, "Legal Requirements for Disaster Recovery Planning: Common Facts and Misconceptions," InformIT, http://www.informit.com/articles/article.aspx?p=777896&rl=1, accessed November 17, 2007.

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California